

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-222360

(P2000-222360A)

(43) 公開日 平成12年8月11日 (2000.8.11)

(51) Int.Cl.	識別記号	F I	テマコード (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 1 7
12/14	3 2 0	12/14	3 2 0 C 5 B 0 5 8
13/00	3 5 4	13/00	3 5 4 Z 5 B 0 8 5
G 0 6 K 17/00		G 0 6 K 17/00	T 5 B 0 8 9
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 A 5 J 1 0 4
審査請求 未請求 請求項の数29 O L (全 48 頁)			

(21) 出願番号 特願平11-24446

(22) 出願日 平成11年2月1日 (1999.2.1)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 柴田 顕男

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72) 発明者 高山 久

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(74) 代理人 100099254

弁理士 役 昌明 (外3名)

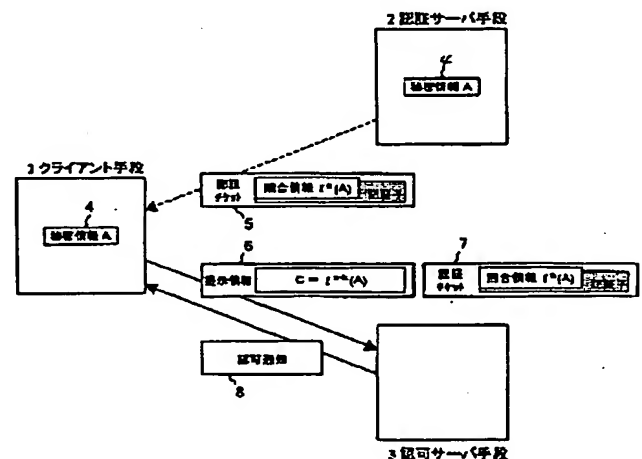
最終頁に続く

(54) 【発明の名称】 認証方法、認証システム及び認証処理プログラム記録媒体

## (57) 【要約】

【課題】 1回のユーザ認証で複数回のアクセスを許可するシングルサインオン型認証において、少ない計算量で正当なアクセスを判別し、不正なアクセスを排除する。

【解決手段】 クライアント手段1と認証サーバ手段2とで秘密情報4を共有する。認証サーバ手段2は秘密情報4に不可逆演算  $f$  を  $n$  回行った照合情報を含んだ認証チケット5を発行する。クライアント手段1はこの認証チケットとともに、秘密情報4に不可逆演算  $f$  を  $n-k$  回行った提示情報を認可サーバ手段3に示す。認可サーバ手段3はこの提示情報に不可逆演算  $f$  を  $k$  回行って、照合情報と一致するかをチェックする。 $k$  を1から  $n$  まで増加させることにより、過去の提示情報から次の提示情報を計算されることなく、最大  $n$  回のアクセスに認証チケット5が使用できる。



## 【特許請求の範囲】

【請求項1】 認証チケットを発行する認証サーバ手段と、認証チケットの利用を認可する認可サーバ手段と、前記認証サーバ手段に認証チケットを要求し、前記認可サーバ手段に認証チケットの利用認可を要求するクライアント手段とを備える認証システムにおいて、有効回数が $n$  ( $n$ は正整数)である認証チケットを保持し、これを示して利用認可を求めるクライアント手段と、これを受けて前記クライアント手段に提示情報を要求し前記認証チケットと照合して利用を認可する認可サーバ手段とを具備し、前記認証チケットは、チケット識別子と照合情報と有効回数とを含み、且つ、認証子が付与されており、前記照合情報は、前記認証サーバ手段と前記クライアント手段とが共有する秘密情報に所定の不可逆演算を $n$ 回施したものであり、前記認証チケットの使用回数が $k$  ( $k$ は $n$ 以下の正整数)であるときの前記提示情報は、前記秘密情報に前記所定の不可逆演算を $n-k$ 回施したものであることを特徴とする認証システム。

【請求項2】 前記認証サーバ手段が、ユーザ認証情報を管理し、前記クライアント手段との間でユーザ認証手順を実行して前記認証チケットを発行することを特徴とする請求項1に記載の認証システム。

【請求項3】 前記認証サーバ手段が、ユーザ認証手順において乱数を生成し、これを示して前記クライアント手段に認証提示情報を要求し、前記秘密情報は、前記ユーザ認証情報と前記乱数との連結に前記所定の不可逆演算を1回以上施したものであり、前記認証提示情報は、前記秘密情報に前記所定の不可逆演算を $n$ 回施したものであることを特徴とする請求項2に記載の認証システム。

【請求項4】 前記認証サーバ手段が、ユーザ認証手順において乱数を生成し、これを示してクライアント手段に認証提示情報を要求し、前記認証提示情報が、前記ユーザ認証情報及び前記乱数との連結に前記所定の不可逆演算を1回以上施したものと前記クライアント手段が生成した認証用乱数との排他的論理和演算結果であり、前記秘密情報が、前記認証提示情報から逆算される前記認証用乱数であることを特徴とする請求項2に記載の認証システム。

【請求項5】 前記ユーザ認証情報が、ユーザにより入力されるパスワードであることを特徴とする請求項2から4のいずれかに記載の認証システム。

【請求項6】 前記ユーザ認証情報が、秘密裏に保持された共通鍵方式暗号鍵であることを特徴とする請求項2から4のいずれかに記載の認証システム。

【請求項7】 前記認証子が、メッセージ認証コードであることを特徴とする請求項1から6のいずれかに記載の認証システム。

【請求項8】 前記認証子が、デジタル署名であること

を特徴とする請求項1から6のいずれかに記載の認証システム。

【請求項9】 前記所定の不可逆演算が、一方向性ハッシュ演算であることを特徴とする請求項1から8のいずれかに記載の認証システム。

【請求項10】 前記認証チケットが、サーバ識別子を含むことを特徴とする請求項1から9のいずれかに記載の認証システム。

【請求項11】 前記認証チケットが、発行日時を含むことを特徴とする請求項1から10のいずれかに記載の認証システム。

【請求項12】 前記認証チケットが、発行者識別子を含み、前記認可サーバ手段が、利用認可するとともに前記認証チケットの照合情報と有効回数と発行日時と発行者識別子と認証子とを更新し、前記照合情報が、前記秘密情報に前記所定の不可逆演算を $n-k$ 回施したものに更新され、前記有効回数が $n-k$ に更新されることを特徴とする請求項11に記載の認証システム。

【請求項13】 前記認可サーバ手段が、前記認証チケットの使用回数を管理しており、これを示して提示情報を要求することを特徴とする請求項1から12のいずれかに記載の認証システム。

【請求項14】 前記クライアント手段が、前記認証チケットの使用回数を管理しており、前記認証チケットとともにこれを示して利用認可を求めることを特徴とする請求項1から12のいずれかに記載の認証システム。

【請求項15】 複数の前記認可サーバ手段と、前記認証チケットの使用回数を管理する認証チケット管理手段とを備えており、前記クライアント手段は、前記認証チケットの使用回数を管理しており、前記認証チケットとともにこれを示して利用認可を求めるものであり、前記認証サーバ手段は、前記認証チケットを発行するとともに前記認証チケット管理手段に前記認証チケットの発行登録を指示し、前記認可サーバ手段は、前記認証チケットの提示を受けて前記認証チケット管理手段に前記認証チケットの履歴更新を指示し、前記認証チケット管理手段より拒絶通知を受けた場合には利用認可しないことを特徴とする請求項1から11のいずれかに記載の認証システム。

【請求項16】 前記認可サーバ手段を複数備え、前記クライアント手段は、前記認証チケットの使用回数を管理しており、前記認証チケットとともにこれを示して利用認可を求めるものであり、前記認証サーバ手段は、前記認証チケットを発行するとともに発行履歴を記憶し、前記認可サーバ手段は、前記認証チケットを更新するとともに更新履歴を記憶し、前記認証チケットの提示を受けて前記認証チケットの発行者識別子が示す前記認証サーバ手段または前記認可サーバ手段に前記認証チケットの履歴を照会し、前記認証サーバ手段または前記認可サーバ手段より拒絶通知を受けた場合には利用認可しない

ことを特徴とする請求項12に記載の認証システム。

【請求項17】 前記認可サーバ手段は、利用認可手順において乱数を生成し、これを示して提示情報を要求するものであり、前記認証チケットの使用回数が $k$ であるときの前記提示情報は前記秘密情報に前記所定の不可逆演算を $n-k$ 回施したものと前記乱数との排他的論理和演算結果であることを特徴とする請求項14から16のいずれかに記載の認証システム。

【請求項18】 認証チケットを発行する認証サーバ手段と、認証チケットの利用を認可する認可サーバ手段と、前記認証サーバ手段に認証チケットを要求し、前記認可サーバ手段に認証チケットの利用認可を要求するクライアント手段とを備える認証システムにおいて、前記クライアント手段が、ユーザ識別子とユーザ認証情報とサーバ識別子と認証チケットの有効回数の入力を得る入力手段と、前記認証サーバ手段より認証チケットを得て保持し、前記認可サーバ手段に提示するチケット保持手段と、前記チケット保持手段より認証チケットの有無情報を得て処理を選択する処理選択手段と、前記入力手段よりユーザ認証情報を得るとともに前記認証サーバ手段より乱数を得て、これらの連結にハッシュ演算を施すハッシュ手段と、前記ハッシュ手段より得たハッシュ値を秘密裏に記憶する機密記憶手段と、前記機密記憶手段よりハッシュ値を取り出して、ユーザ認証手順においては前記入力手段より有効回数 $n$  ( $n$ は正整数)を得て、 $n$ 段のハッシュ演算を施して得た多段ハッシュ値を前記認証サーバ手段に送り、利用認可手順においては前記認可サーバ手段より利用回数 $k$  ( $k$ は $n$ 以下の正整数)を得て、 $n-k$ 段のハッシュ演算を施して得た多段ハッシュ値を前記認可サーバ手段に送る多段ハッシュ手段とを具備し、前記認証サーバ手段が、ユーザ認証情報が蓄積された認証情報蓄積手段と、乱数を生成して前記クライアント手段に送る乱数生成手段と、前記認証情報蓄積手段より得たユーザ認証情報と前記乱数生成手段で生成した乱数との連結に $n+1$ 段のハッシュ演算を行なう第2の多段ハッシュ手段と、前記クライアント手段より得た多段ハッシュ値を前記第2の多段ハッシュ手段で得た多段ハッシュ値と照合する認証照合手段と、有効なチケット識別子を生成するチケット識別子生成手段と、時刻を計時し時刻情報を出力する認証計時手段と、前記チケット識別子生成手段より得たチケット識別子、前記認証照合手段より得た多段ハッシュ値、前記クライアント手段より得たサーバ識別子及び有効回数、前記認証計時手段より得た時刻情報に基づくタイムスタンプ、並びに認証サーバ手段を示す発行者識別子の連結に認証子を付加し、認証チケットとして前記クライアント手段に送る認証子付加手段とを具備し、

前記認可サーバ手段が、前記クライアント手段より得た認証チケットの認証子を検証する認証子検証手段と、時

刻を計時し時刻情報を出力する認可計時手段と、サーバ識別子の妥当性及びタイムスタンプと前記認可計時手段より得た時刻情報との差の有効性をチェックするチケット有効判定手段と、認証チケットのチケット識別子と利用回数と残り利用可能回数とを管理するチケット利用管理手段と、前記チケット利用管理手段より利用回数 $k$ を得て、前記クライアント手段より得た多段ハッシュ値に $k$ 段のハッシュ演算を施して得た二次多段ハッシュ値を出力する第3の多段ハッシュ手段と、前記チケット利用管理手段より得た多段ハッシュ値と前記第3の多段ハッシュ手段より得た二次多段ハッシュ値とを照合する認可照合手段とを具備することを特徴とする認証システム。

【請求項19】 前記認証子付加手段が、サーバ間で共有する共通鍵方式暗号鍵を記憶するサーバ共通鍵記憶手段と、自識別子を記憶する自識別子記憶手段と、チケット識別子と多段ハッシュ値と有効回数とタイムスタンプとサーバ識別子と前記自識別子記憶手段より得た発行者識別子とを連結するデータ連結手段と、前記データ連結手段より得た連結データにハッシュ演算を施す連結データハッシュ手段と、前記サーバ共通鍵記憶手段より得た共通鍵方式暗号鍵を用いて前記連結データハッシュ手段より得たハッシュ値を暗号化して認証子とする共通鍵方式暗号手段と、前記データ連結手段より得た連結データと前記共通鍵方式暗号手段より得た認証子とを連結する認証子連結手段とを具備し、前記認証子検証手段が、サーバ間で共有する共通鍵方式暗号鍵を記憶する第2のサーバ共通鍵記憶手段と、認証チケットを連結データと認証子とに分離する認証子分離手段と、前記認証子分離手段より得た連結データをチケット識別子と多段ハッシュ値と有効回数とタイムスタンプとサーバ識別子と発行者識別子とに分離するデータ分離手段と、前記認証子分離手段より得た連結データにハッシュ演算を施す第2の連結データハッシュ手段と、前記第2のサーバ共通鍵記憶手段より得た共通鍵方式暗号鍵を用いて前記第2の連結データハッシュ手段より得たハッシュ値を暗号化して比較用認証子とする第2の共通鍵方式暗号手段と、前記データ分離手段より得た発行者識別子が有効なサーバ識別子であることをチェックする発行者識別子照合手段と、前記発行者識別子照合手段より得た照合結果が有効を示す場合に前記認証子分離手段より得た認証子と前記第2の共通鍵方式暗号手段より得た比較用認証子とを比較して結果を出力する比較手段とを具備することを特徴とする請求項18に記載の認証システム。

【請求項20】 前記認証子付加手段が、認証サーバの公開鍵方式暗号秘密鍵を秘密裏に記憶する自秘密鍵記憶手段と、自識別子を記憶する自識別子記憶手段と、チケット識別子と多段ハッシュ値と有効回数とタイムスタンプとサーバ識別子と前記自識別子記憶手段より得た発行者識別子とを連結するデータ連結手段と、前記データ連

結手段より得た連結データにハッシュ演算を施す連結データハッシュ手段と、前記自秘密鍵記憶手段より得た公開鍵方式暗号秘密鍵を用いて前記連結データハッシュ手段より得たハッシュ値を暗号化して認証子とする公開鍵方式暗号手段と、前記データ連結手段より得た連結データと前記公開鍵方式暗号手段より得た認証子とを連結する認証子連結手段とを具備し、

前記認証子検証手段が、認証チケットを連結データと認証子とに分離する認証子分離手段と、前記認証子分離手段より得た連結データをチケット識別子と多段ハッシュ値と有効回数とタイムスタンプとサーバ識別子と発行者識別子とに分離し出力するデータ分離手段と、前記認証子分離手段より得た連結データにハッシュ演算を施す第2の連結データハッシュ手段と、有効なサーバの公開鍵方式暗号公開鍵が蓄積され前記データ分離手段より得た発行者識別子に対応する公開鍵方式暗号公開鍵を出力するサーバ公開鍵蓄積手段と、前記サーバ公開鍵蓄積手段より得た公開鍵方式暗号公開鍵を用いて前記認証子分離手段より得た認証子を復号し比較用ハッシュ値とする公開鍵方式復号手段と、前記連結データハッシュ手段より得たハッシュ値と前記公開鍵方式復号手段より得た比較用ハッシュ値とを比較して結果を出力する比較手段とを具備することを特徴とする請求項18に記載の認証システム。

【請求項21】 前記クライアント手段が、認証乱数生成手段と第1の排他的論理和手段とを具備し、前記認証用乱数生成手段は、ユーザ認証手順において認証用乱数を生成し、前記第1の排他的論理和手段は、ユーザ認証手順において前記認証用乱数生成手段より得た認証用乱数と前記ハッシュ手段より得たハッシュ値との排他的論理和演算を行なって得た攪乱ハッシュ値を前記認証サーバ手段に送り、前記機密記憶手段は、前記認証用乱数生成手段より得た認証用乱数を秘密裏に記憶し、前記多段ハッシュ手段は、前記機密記憶手段より認証用乱数を取り出して、利用認可手順において前記認可サーバ手段より利用回数 $k$ を得て、 $n-k$ 段のハッシュ演算を施して得た多段ハッシュ値を前記認可サーバ手段に送り、前記認証サーバ手段が、前記認証照合手段に代わり第2のハッシュ手段及び第2の排他的論理和手段を具備し、前記第2のハッシュ手段は、前記認証情報蓄積手段より得たユーザ認証情報と前記乱数生成手段で生成した乱数との連結にハッシュ演算を施し、前記第2の排他的論理和手段は、前記第2のハッシュ手段より得たハッシュ値と前記クライアント手段より得た攪乱ハッシュ値との排他的論理和演算を行なって認証用乱数を取得し、前記第2の多段ハッシュ手段は、前記第2の排他的論理和手段より得た認証用乱数に $n$ 段のハッシュ演算を行ない、前記認証子付加手段は、前記チケット識別子生成手段より得たチケット識別子、前記第2の多段ハッシュ手段より得た多段ハッシュ値、前記クライアント手段より得たサ

ーバ識別子及び有効回数、前記認証計時手段より得た時刻情報に基づくタイムスタンプ、並びに認証サーバ手段を示す発行者識別子の連結に認証子を付加し、認証チケットとして前記クライアント手段に送ることを特徴とする請求項18から20のいずれかに記載の認証システム。

【請求項22】 前記認可サーバ手段が、前記第3の多段ハッシュ手段に代わり第3のハッシュ手段及び第2の認証子付加手段を具備し、前記第3のハッシュ手段は、前記クライアント手段より得た多段ハッシュ値にハッシュ演算を施して得た二次多段ハッシュ値を出力し、前記認可照合手段は、前記チケット利用管理手段より得た多段ハッシュ値と前記第3のハッシュ手段より得た二次多段ハッシュ値とを照合し、前記第2の認証子付加手段は、前記チケット利用管理手段より得たチケット識別子、サーバ識別子及び残り利用回数、前記クライアント手段より得た多段ハッシュ値、前記認可計時手段より得た時刻情報に基づくタイムスタンプ、並びに認可サーバ手段を示す発行者識別子の連結に認証子を付加し、認証チケットとして前記クライアント手段に送ることを特徴とする請求項18から21のいずれかに記載の認証システム。

【請求項23】 1つ以上の認可サーバ手段と、認証チケットの発行及び利用状況を管理する認証チケット管理手段とを具備し、前記認証チケット管理手段が、前記認証サーバ手段より得た認証チケット発行登録指示をもとにチケット識別子と有効回数と残り利用回数との組を管理して、前記認可サーバ手段より得た認証チケット履歴更新指示との整合性をチェックし、不整合の場合には前記認可サーバ手段に認証チケット拒絶通知を送り、前記認証サーバ手段が、チケット登録指示手段を具備し、前記チケット登録指示手段は、前記チケット識別子生成手段より得たチケット識別子と前記クライアント手段より得たサーバ識別子及び有効回数とから認証チケット発行登録指示を生成して前記認証チケット管理手段に送り、

前記クライアント手段が、前記チケット保持手段に代わるチケット保持管理手段と、第1の排他的論理和手段とを具備し、前記チケット保持管理手段は、前記認証サーバ手段より認証チケットを得て保持するとともに利用回数を管理して、前記認可サーバ手段にそれらを提示し、前記多段ハッシュ手段は、前記機密記憶手段よりハッシュ値を取り出して、ユーザ認証手順においては $n$ 段のハッシュ演算を施して得た多段ハッシュ値を前記認証サーバ手段に送り、利用認可手順においては前記チケット保持管理手段より得た利用回数 $k$ を得て、 $n-k$ 段のハッシュ演算を施して得た多段ハッシュ値を前記第1の排他的論理和手段に送り、前記第1の排他的論理和手段は、前記多段ハッシュ手段より得た多段ハッシュ値と前記認可サーバ手段より得た乱数との排他的論理和演算を行な

って結果の攪乱多段ハッシュ値を前記認可サーバ手段に送り、

前記認可サーバ手段が、チケット利用管理手段に代わるチケット更新指示手段と、第2の乱数生成手段と、第2の排他的論理和手段とを具備し、前記チケット更新指示手段は、前記チケット有効判定手段より得た判定結果が有効を示す場合に前記認証子検証手段より得たチケット識別子及びサーバ識別子と前記クライアント手段より得た利用回数とから認証チケット履歴更新指示を生成して前記認証チケット管理手段に送り、前記認証チケット管理手段より認証チケット拒絶通知が返されなかった場合に前記クライアント手段より得た利用回数 $k$ と前記認証子検証手段より得た多段ハッシュ値とを出力し、前記第2の乱数生成手段は、乱数を生成して前記クライアント手段及び前記第2の排他的論理和手段に送り、前記第2の排他的論理和手段は、前記第2の乱数生成手段より得た乱数と前記クライアント手段より得た攪乱多段ハッシュ値との排他的論理和演算を行なって多段ハッシュ値を取得し、前記第3の多段ハッシュ手段は、前記第2の排他的論理和手段より得た多段ハッシュ値に $k$ 段のハッシュ演算を施して得た二次多段ハッシュ値を出力し、前記認証チケット管理手段は、前記認証サーバ手段より得た認証チケット発行登録指示をもとにチケット識別子と有効回数と残り利用回数との組を管理し、前記認可サーバ手段より得た認証チケット履歴更新指示との整合性をチェックし、不整合の場合には前記認可サーバ手段に認証チケット拒絶通知を送ることを特徴とする請求項18から21のいずれかに記載の認証システム。

【請求項24】 認可サーバ手段を1つ以上具備し、前記認証サーバ手段が、チケット発行管理手段を具備し、前記チケット発行管理手段は、前記チケット識別子生成手段より得たチケット識別子と前記クライアント手段より得たサーバ識別子及び有効回数とを管理し、前記認可サーバ手段より得たチケット利用照会をもとにチケット識別子を検索して利用回数の整合性をチェックし、不整合の場合には前記認可サーバ手段に認証チケット拒絶通知を送り、

前記クライアント手段が、前記チケット保持手段に代わるチケット保持管理手段と、第1の排他的論理和手段とを具備し、前記チケット保持管理手段は、前記認証サーバ手段より認証チケットを得て保持するとともに利用回数を管理して、前記認可サーバ手段にそれらを提示し、前記多段ハッシュ手段は、前記機密記憶手段よりハッシュ値を取り出して、ユーザ認証手順においては $n$ 段のハッシュ演算を施して得た多段ハッシュ値を前記認証サーバ手段に送り、利用認可手順においては前記チケット保持管理手段より得た利用回数 $k$ を得て、 $n-k$ 段のハッシュ演算を施して得た多段ハッシュ値を前記第1の排他的論理和手段に送り、前記第1の排他的論理和手段は、前記多段ハッシュ手段より得た多段ハッシュ値と前記認

可サーバ手段より得た乱数との排他的論理和演算を行なって結果の攪乱多段ハッシュ値を前記認可サーバ手段に送り、

前記認可サーバ手段が、前記チケット利用管理手段に代わるチケット更新管理手段と、第2の乱数生成手段及び第2の排他的論理和手段とを具備し、前記チケット更新管理手段は、前記チケット有効判定手段より得た判定結果が有効を示す場合に前記認証子検証手段より得たチケット識別子及びサーバ識別子と前記クライアント手段より得た利用回数とからチケット利用照会を生成し、発行者識別子が示す前記認証サーバ手段または第2の認可サーバ手段に対して送り、前記認証サーバ手段または前記第2の認可サーバ手段より認証チケット拒絶通知が返されなかった場合に、前記クライアント手段より得た利用回数と前記認証子検証手段より得た多段ハッシュ値とを出力するとともに、チケット識別子、サーバ識別子及び残り利用回数を管理して、前記第2の認可サーバ手段よりチケット利用照会を受けた場合に利用回数の整合性をチェックし、不整合の場合には前記第2の認可サーバ手段に認証チケット拒絶通知を送り、前記第2の乱数生成手段は、乱数を生成して前記クライアント手段及び前記第2の排他的論理和手段に送り、前記第2の排他的論理和手段は、前記第2の乱数生成手段より得た乱数と前記クライアント手段より得た攪乱多段ハッシュ値との排他的論理和演算を行なって多段ハッシュ値を取得し、前記第2のハッシュ手段は、前記第2の排他的論理和手段より得た多段ハッシュ値にハッシュ演算を施して得た二次多段ハッシュ値を出力し、前記第2の認証子付加手段は、前記チケット管理手段より得たチケット識別子、サーバ識別子及び残り利用回数、前記第2の排他的論理和手段より得た多段ハッシュ値、前記認可計時手段より得た時刻情報に基づくタイムスタンプ、並びに認可サーバ手段を示す発行者識別子の連結に認証子を付加し、認証チケットとして前記クライアント手段に送ることを特徴とする請求項22に記載の認証システム。

【請求項25】 認証チケットを発行する認証サーバ手段と、認証チケットの利用を認可する認可サーバ手段と、前記認証サーバ手段に認証チケットを要求し、前記認可サーバ手段に認証チケットの利用認可を要求するクライアント手段とを備える認証システムの認証方法において、

認証サーバ手段からクライアント手段に、認証サーバ手段とクライアント手段とが共有する秘密情報に所定の不可逆演算を $n$  ( $n$ は正整数) 回施した照合情報を含む、有効回数が $n$ である認証チケットを発行し、クライアント手段は、前記認証チケットを認可サーバ手段に示して利用認可を求め、認可サーバ手段の提示情報の要求に対して、クライアント手段は、前記認証チケットの使用回数が $k$  ( $k$ は $n$ 以下の正整数) であるとき、前記秘密情報に前記所定の不可逆演算を $n-k$  回施した演算結果を



前記提示情報として提示し、認可サーバ手段は、前記提示情報に前記所定の不可逆演算を $k$ 回施し、その演算結果と前記照合情報との一致を識別することを特徴とする認証方法。

【請求項26】 認証チケットを発行する認証サーバ手段と、認証チケットの利用を認可する認可サーバ手段と、前記認証サーバ手段に認証チケットを要求し、前記認可サーバ手段に認証チケットの利用認可を要求するクライアント手段とを備える認証システムの認証方法において、

認証サーバ手段からクライアント手段に、認証サーバ手段とクライアント手段とが共有する秘密情報に所定の不可逆演算を $n$  ( $n$ は正整数)回施した照合情報を含む、有効回数が $n$ である認証チケットを発行し、クライアント手段は、前記認証チケットを認可サーバ手段に示して利用認可を求め、認可サーバ手段の提示情報の要求に対して、クライアント手段は、前記認証チケットの使用回数が $k$  ( $k$ は $n$ 以下の正整数)であるとき、前記秘密情報に前記所定の不可逆演算を $n-k$ 回施した演算結果を前記提示情報として提示し、認可サーバ手段は、前記提示情報に前記所定の不可逆演算を1回施し、その演算結果と前記照合情報との一致を識別するとともに、前記認証チケットに含まれる照合情報を前記秘密情報に前記所定の不可逆演算を $n-k$ 回施した演算結果に更新することを特徴とする認証方法。

【請求項27】 前記認証サーバ手段が、認証チケットを要求するクライアント手段に乱数を示して認証提示情報を要求し、クライアント手段は、ユーザ認証情報と前記乱数との連結に前記所定の不可逆演算を $n+1$ 回施した演算結果を前記認証提示情報として提示し、認証サーバ手段は、保持しているユーザ認証情報と前記乱数との連結に前記所定の不可逆演算を $n+1$ 回施して、その演算結果と前記認証提示情報との一致を確認すると、前記ユーザ認証情報と前記乱数との連結に前記所定の不可逆演算を1回施した演算結果を前記秘密情報として、これに所定の不可逆演算を $n$  ( $n$ は正整数)回施した前記照合情報を含む認証チケットを発行することを特徴とする請求項25または26に記載の認証方法。

【請求項28】 前記認証サーバ手段が、認証チケットを要求するクライアント手段に乱数を示して認証提示情報を要求し、クライアント手段は、ユーザ認証情報と前記乱数との連結に前記所定の不可逆演算を1回以上施したものとクライアント手段が生成した認証用乱数との排他的論理和演算結果を前記認証提示情報として提示し、認証サーバ手段は、保持しているユーザ認証情報と前記乱数とを用いて前記認証提示情報から前記認証用乱数を逆算し、前記認証用乱数を前記秘密情報として、これに所定の不可逆演算を $n$  ( $n$ は正整数)回施した前記照合情報を含む認証チケットを発行することを特徴とする請求項25または26に記載の認証方法。

【請求項29】 請求項1から24のいずれかに記載の認証システムで実行される認証方法または請求項25から28のいずれかに記載の認証方法の処理プログラムを、電子計算機が読取り可能な形式で記録した、認証処理プログラム記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、クライアント装置がサーバ装置にアクセスすることの妥当性を判断する1回の処理をもって複数回のアクセスを許可する、シングルサインオン型の認証方法及び認証システムに関し、特に、クライアント装置での暗号処理を不要にし、計算処理能力が低い装置でも処理できるようにしたものである。

【0002】

【従来の技術】近年、デジタル通信技術の発達にともない、ネットワークを介して接続されたサーバ装置及びクライアント装置から構成されるサーバ・クライアント型システムが一般的なものとなって来た。そのようなサーバ・クライアント型システムにおいては、クライアント装置及びそのユーザがサーバ装置にアクセスする正当な権限を有することを確認し、不正なアクセスが行なわれないようにすることが重要である。このアクセス権限を確認する認証方法としては、パスワード入力によるものが良く知られるが、アクセスする度にパスワード入力を求める方法は安全である反面ユーザにとっては不便であるため、利便性を向上させたシングルサインオン型の認証方法が利用されるようになって来た。このようなシングルサインオン型の認証方法としては、例えば、Kerberos認証システムで用いられるTTP (Trusted Third-party Protocol) が一般に知られている。

【0003】以下、従来のシングルサインオン型の認証方法について図面を参照しながら説明する。図23は従来のシングルサインオン型の認証方法の概要を示す概念図であり、図24はプロトコルを示すプロトコルシーケンス図である。図23及び図24において、81はユーザインタフェースを持つクライアント手段、82はユーザ認証を行なう認証サーバ手段、83はアクセス権限を判断して利用認可を行なう認可サーバ手段である。

【0004】クライアント手段81と認証サーバ手段82とのユーザ認証手順においては、ユーザインタフェースを介して入力されたユーザ識別子UIDとサーバ識別子SIDとを認証提示情報としてともなった認証要求Authenticate Request801をクライアント手段81が認証サーバ手段82に送り、これに対し認証サーバ手段82がパスワードPWを鍵として暗号化されたセッション鍵SKをとともなった認証応答Authorize Request802を認証チケットTicket803とともに送り返す。

【0005】さらに、クライアント手段81と認可サーバ手段83との利用認可手順においては、クライアント手段

81がセッション鍵SKで暗号化されたユーザ識別子UIDとタイムスタンプTSkとを提示情報としてともなった認可要求Authorize Request804を認証チケットTicket805とともに認可サーバ手段83に送り、これに対し認可サーバ手段83は認証要求Authorize Request804における提示情報と認証チケットTicket805とを検証して、正当と認めれば認可通知Result806を送り返すものである。

【0006】以上のようなプロトコルシーケンスを持つ従来のシングルサインオン型の認証方法において、以下その構成について図25を参照しながら説明する。図25は、従来のシングルサインオン型の認証方法の構成を示す機能ブロック図である。図25においても、81はユーザインタフェースを持つクライアント手段、82はユーザ認証を行なう認証サーバ手段、83はアクセス権限を判断して利用認可を行なう認可サーバ手段である。

【0007】クライアント手段81は、データの送受信を行なう第1の送受信手段311と、ユーザからの入力を得る入力手段811と、受信したセッション鍵を復号するセッション鍵復号手段812と、受信した認証チケットを保持するチケット保持手段314と、認証チケットの保持状態に応じて処理を選択する処理選択手段315と、復号したセッション鍵を秘密裏に記憶する機密記憶手段316と、時刻を計時する証明計時手段813と、セッション鍵を用いて認証済み証明情報を暗号化する証明情報暗号手段814とから構成される。

【0008】また、認証サーバ手段82は、データの送受信を行なう第2の送受信手段321と、時刻を計時する認証計時手段322と、パスワード等のユーザ認証情報が蓄積された認証情報蓄積手段323と、ユーザ認証処理毎に暗号鍵を生成するセッション鍵生成手段821と、パスワードを用いてセッション鍵を暗号化するセッション鍵暗号手段822と、セッション鍵を用いて認証チケットを暗号化するチケット暗号手段823とから構成される。

【0009】また、認可サーバ手段83は、データの送受信を行なう第3の送受信手段331と、時刻を計時する認可計時手段332と、認証チケットを復号するチケット復号手段831と、認証チケットの有効性判定を行なうチケット有効判定手段832と、認証済み証明情報を復号化する証明情報復号手段833と、認証済み証明情報の有効性判定を行なう証明情報有効判定手段834と、認証チケットの内容と認証済み証明情報の内容とを比較照合する認可照合手段835とから構成される。

【0010】以上のように構成された従来のシングルサインオン型の認証方法において、以下その動作について図26を参照しながら説明する。まず、クライアント手段81において、ユーザ自身を示すユーザ識別子UIDと認証サーバ手段82にあらかじめ登録されたユーザ認証用のパスワードPWと利用認可を得る対象のサーバ識別子SIDとがユーザ入力800として入力手段811に入力される(ST3101、ST8101)。入力手段811は、

ユーザ入力800を一時保持するとともにサーバ識別子3101を取出してチケット保持手段314に送る。チケット保持手段314は、サーバ識別子3101に対応する認証チケットデータを検索して(ST3102)、検索結果通知3102を処理選択手段315に送る。処理選択手段315は、検索結果通知3102が無しを示す場合には、ユーザ認証処理起動通知8101を前記入力手段811に送り、有りを示す場合には、利用認可手順起動通知8102を前記チケット保持手段314、機密記憶手段316及び証明情報暗号手段814に送る(ST3103)。

【0011】前記入力手段811は、ユーザ認証起動通知8101が与えられると、一時保持したユーザ入力800から取出した、ユーザ識別子とサーバ識別子との組8103を第1の送受信手段311を介して認証要求Authenticate Request801として認証サーバ手段82に送り(ST8102)、ユーザ識別子8104を証明情報暗号手段814に送り、パスワード8105をセッション鍵復号手段812に送る。

【0012】認証サーバ手段82においては、認証要求Authenticate Request801は第2の送受信手段321で受信され、取出されたユーザ識別子8201が認証情報蓄積手段323及びチケット暗号手段823に送られ、サーバ識別子8202がチケット暗号手段823に送られる(ST8201)。認証情報蓄積手段323は、ユーザ識別子8201に対応するパスワードを検索して(ST8202)、有りの場合にはパスワード8203をセッション鍵暗号手段822に送り、検索結果通知8204をセッション鍵生成手段821及びセッション鍵暗号手段822に送る(ST8203)。セッション鍵生成手段821は、検索結果通知8204が有りを示す場合に、新たにランダムなセッション鍵8205を生成してセッション鍵暗号手段822及びチケット暗号手段823に送る(ST8204)。セッション鍵暗号手段822は、検索結果通知8204が有りを示す場合に、セッション鍵8205をパスワード8203を用いて暗号化した暗号化セッション鍵8206を生成し(ST8205)、これを第2の送受信手段321を介して認証応答Authenticate Response802としてクライアント手段81に送る(ST8207)。認証計時手段322は、現在時刻を計時しており、現在時刻に基づくタイムスタンプ3212をチケット暗号手段823に供給している。チケット暗号手段823は、内部に保持しサーバ識別子8202に対応したサーバ共通鍵を用いて、ユーザ識別子8201とサーバ識別子8202とタイムスタンプ3212とセッション鍵8205とを暗号化した認証チケットデータ8207を生成し(ST8202、ST8206)、これを第2の送受信手段321を介して認証チケットTicket803としてクライアント手段81に送る(ST8207)。

【0013】クライアント手段81においては、認証応答Authenticate Response802は第1の送受信手段311を介して暗号化セッション鍵8106としてセッション鍵復号手段812に送られ、認証チケットTicket803は第1の送受信手段311を介して認証チケットデータ8108として前記チ

チケット保持手段314に送られる（ST8103）。前記チケット保持手段314は認証チケットデータ8108をサーバ識別子3101と対応づけて保持する（ST3112）。セッション鍵復号手段812は、暗号化セッション鍵8106をパスワード8105を用いて復号化する（ST8104）。従って、正しいパスワードが入力された場合にのみ正しいセッション鍵を得ることができる。セッション鍵復号手段812で得られたセッション鍵8107は機密記憶手段316に送られ記憶される。

【0014】機密記憶手段316は、セッション鍵8107を秘密裏に記憶して所定のアクセスのみ許可するもので（ST8105）、利用認可手順起動通知8102が与えられた場合に、記憶したセッション鍵8109を証明情報暗号手段814に送る。証明計時手段813は、現在時刻を計時しており、現在時刻に基づくタイムスタンプ8110を証明情報暗号手段814に供給している。証明情報暗号手段814は、利用認可手順起動通知8102が与えられると、ユーザ識別子8104とタイムスタンプ8110とをセッション鍵8109を用いて暗号化した認証済み証明情報8111を生成し（ST8106）、これを第1の送受信手段311を介して認可要求Authorize Request804として認可サーバ手段83に送る（ST8107）。前記チケット保持手段314は、利用認可手順起動通知8102が与えられると、サーバ識別子3101に対応する保持した認証チケットデータ8112を、第1の送受信手段311を介して認証チケットTicket805として認可サーバ手段83に送る（ST8107）。

【0015】認可サーバ手段83においては、認可要求Authorize Request804は第3の送受信手段331を介して認証済み証明情報8308として証明情報復号手段833に送られ、認証チケットTicket805は第3の送受信手段331を介して認証チケットデータ8301としてチケット復号手段831に送られる（ST8301）。チケット復号手段831は、認証チケットデータ8301を内部に保持した自サーバ共通鍵を用いて復号化して、得られたユーザ識別子8302とサーバ識別子8303とタイムスタンプ8304とをチケット有効判定手段832に送り、セッション鍵8305を証明情報復号手段833に送る（ST8302）。認可計時手段332は、現在時刻を計時しており、現在時刻情報8306をチケット有効判定手段832及び証明情報有効判定手段834に供給している。チケット有効判定手段832は、サーバ識別子8303と内部に保持した自サーバ識別子との一致判定を行なうとともに、タイムスタンプ8304と現在時刻情報8306との差が所定の有効期限の範囲内であることをチェックして、いずれも真である場合にユーザ識別子8302をチケットユーザ識別子8307として認可照合手段835に送る（ST3306、ST3307）。証明情報復号手段833は、認証済み証明情報8308をセッション鍵8305を用いて復号化して、得られたユーザ識別子8309とタイムスタンプ8310とを証明情報有効判定手段834に送る（ST8303）。認証済み証明情報はクライアント手段でセ

ッション鍵を用いて暗号化されているので、クライアント手段で正しいセッション鍵が用いられた場合にのみ、ここで正しいユーザ識別子とタイムスタンプとが得られる。証明情報有効判定手段834は、タイムスタンプ8310と現在時刻情報8306との差が所定の時間差の範囲内であることをチェックして、真である場合にユーザ識別子8309を証明ユーザ識別子8311として認可照合手段835に送る（ST8304、ST8305）。認可照合手段835は、チケットユーザ識別子8307と証明ユーザ識別子8311との一致判定を行ない（ST8306）、真であるならば認可通知8312を、第3の送受信手段331を介して認可通知Result806としてクライアント手段81に送り（ST8307、ST3317）、クライアント手段81において受信される（ST3118）。このとき、一致判定が真となった場合、ユーザ識別子とタイムスタンプとが正しく得られており、これはクライアント手段で正しいセッション鍵が用いられたことを示しており、これは正しいパスワードが入力されたことを意味するので、ユーザ認証結果と利用認可結果とが一致することになる。

【0016】

【発明が解決しようとする課題】しかしながら、上記従来の構成では、多大な計算量を必要とする暗号処理を多用しており、特に利用認可処理のたびにクライアント側で暗号処理を行なう必要があるため、クライアント側が携帯型情報端末やスマートフォンのような計算処理能力の低い装置である場合には、実用的な処理時間で利用認可処理を行なうことが困難であるという課題を有していた。

【0017】また、上記従来の構成では、1つの認証チケットの使用回数を制限しておらず有効期限を設けているのみであるため、第三者により盗聴された認証チケットの暗号が万一解読されて不正なアクセスが行なわれたとしても、発見されずに終わってしまう可能性が高いという課題も有していた。

【0018】本発明は、こうした従来の課題を解決するものであり、クライアント側での暗号処理を必要とせず、計算処理能力の低い装置であっても実用的な処理時間で利用認可処理を行なうことができ、認証チケットの使用回数を容易に管理することができる、シングルサインオン型の認証方法及び認証システムを提供することを目的とする。

【0019】

【課題を解決するための手段】この課題を解決するために、本発明は、第1に、有効回数が $n$ （ $n$ は正整数）である認証チケットを保持し、これを示して利用認可を求めるクライアント手段と、これを受けて提示情報を要求し前記認証チケットと照合して利用認可する認可サーバ手段と設け、前記認証チケットは、チケット識別子と照合情報と有効回数と発行日時とサーバ識別子とを含み認証子が付与されたものであり、前記照合情報は、前記認



証チケットの発行者と前記クライアント手段とが共有する秘密情報に所定の不可逆演算を $n$ 回施したものであり、前記認証チケットの使用回数が $k$  ( $k$ は $n$ 以下の正整数)であるときの前記提示情報は、前記秘密情報に前記所定の不可逆演算を $n-k$ 回施したものであることを特徴としている。

【0020】これにより、クライアント側での暗号処理を必要とせず、認証チケットの使用回数を容易に管理して二重使用を排除することができる、シングルサインオン型の認証方法及び認証システムが得られる。

【0021】第2に、前記認証サーバ手段は、ユーザ認証手順において乱数を生成し、これを示してクライアント手段に認証提示情報を要求するものであり、前記秘密情報は、前記ユーザ認証情報と前記乱数との連結に前記所定の不可逆演算を1回以上施したものであり、前記認証提示情報は、前記秘密情報に前記所定の不可逆演算を $n$ 回施したものであることを特徴としている。

【0022】これにより、上記効果に加えて、ユーザ認証手順においてもクライアント側での暗号処理を必要としないうえ、認証提示情報の演算処理と提示情報の演算処理とが共通化できる、シングルサインオン型の認証方法及び認証システムが得られる。

【0023】第3に、前記認証サーバ手段は、ユーザ認証手順において乱数を生成し、これを示してクライアント手段に認証提示情報を要求するものであり、前記認証提示情報は、前記ユーザ認証情報及び前記乱数との連結に前記所定の不可逆演算を1回以上施したものとクライアント手段が生成した認証用乱数との排他的論理和演算結果であり、前記秘密情報は、前記認証提示情報から逆算される前記認証用乱数であることを特徴としている。

【0024】これにより、上記効果に加えて、認証チケットに含まれる照合情報がユーザ認証情報と無関係となるため認証チケットからユーザ認証情報が推測される可能性すらない、より安全なシングルサインオン型の認証方法及び認証システムが得られる。

【0025】第4に、前記所定の不可逆演算が一方向性ハッシュ演算であることを特徴としている。

【0026】これにより、上記効果に加えて、クライアント側が計算処理能力の低い装置であっても実用的な処理時間で利用認可処理を行なうことができる、シングルサインオン型の認証方法及び認証システムが得られる。

【0027】第5に、前記認証チケットは発行者識別子を含み、前記認可サーバ手段は、利用認可するとともに前記認証チケットの照合情報と有効回数と発行日時と発行者識別子と認証子とを更新するものであり、前記照合情報は、前記秘密情報に前記所定の不可逆演算を $n-k$ 回施したもので更新され、前記有効回数は、 $n-k$ で更新されることを特徴としている。

【0028】これにより、上記効果に加えて、認証チケットは使用すごとに更新され、特にタイムスタンプが

更新されるため有効判定における有効期限をより短く設定できるので、第三者による不正使用の可能性をより小さくでき、さらに利用認可の応答時間を短縮できる、シングルサインオン型の認証方法及び認証システムが得られる。

【0029】第6に、前記クライアント手段は、前記認証チケットの使用回数を管理しており、前記認証チケットとともにこれを示して利用認可を求めるものであり、前記認可サーバ手段を複数備え、前記認証チケットの使用回数を管理する認証チケット管理手段を備えており、前記認証サーバ手段は、前記認証チケットを発行するとともに前記認証チケット管理手段に前記認証チケットの発行登録を指示し、前記認可サーバ手段は、前記認証チケットの提示を受けて前記認証チケット管理手段に前記認証チケットの履歴更新を指示し、前記認証チケット管理手段より拒絶通知を受けた場合には利用認可しないことを特徴としている。

【0030】これにより、上記効果に加えて、認証チケットが更新されないシステムにおいて、認証チケットを複数の認可サーバに対して共通に用いることが可能となるため、より利便性の高い、シングルサインオン型の認証方法及び認証システムが得られる。

【0031】第7に、前記クライアント手段は、前記認証チケットの使用回数を管理しており、前記認証チケットとともにこれを示して利用認可を求めるものであり、前記認可サーバ手段を複数備え、前記認証サーバ手段は、前記認証チケットを発行するとともに発行履歴を記憶し、前記認可サーバ手段は、前記認証チケットを更新するとともに更新履歴を記憶し、前記認証チケットの提示を受けて前記認証チケットの発行者識別子が示す前記認証サーバ手段または前記認可サーバ手段に前記認証チケットの履歴を照会し、前記認証サーバ手段または前記認可サーバ手段より拒絶通知を受けた場合には利用認可しないことを特徴としている。

【0032】これにより、上記効果に加えて、認証チケットが更新されるシステムにおいて、認証チケットの利用を分散管理できるため1個所の管理リソースをより少なくできる、シングルサインオン型の認証方法及び認証システムが得られる。

【0033】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照しながら説明する。

【0034】(第1の実施の形態) 第1の実施形態の認証システムは、図1に示すように、ユーザインタフェースを持つクライアント手段1と、ユーザ認証を行なう認証サーバ手段2と、クライアント手段1のアクセス権限を判断して利用認可を行なう認可サーバ手段3とから成る。クライアント手段1には、例えば汎用コンピュータ、携帯情報端末、スマートフォンなどが使用でき、認証サーバ手段2には、例えば汎用コンピュータ、専用認

証サーバ装置などが使用でき、また、認可サーバ手段3には、汎用コンピュータ、専用認可サーバ装置、専用情報提供装置などが使用できる。

【0035】クライアント手段1と認可サーバ手段3との間は有線または無線通信ネットワークにより接続される。クライアント手段1と認証サーバ手段2との間は必ずしも通信ネットワークで接続されていないが、秘密情報4を共有している必要がある。この秘密情報4としては、例えばパスワード、共通鍵方式暗号鍵、またはそれらから算出される計算値などが用いられる。

【0036】クライアント手段1は、利用認可手順で用いる認証チケット5を保持している。これは認証サーバ手段2がクライアント手段1に対して発行したものであり、認証サーバ手段2は、秘密情報4に不可逆演算 $f$ を $n$ 回（ $n$ は認証チケットの有効回数）行なった結果を照合情報とし、これに認証子を付加して認証チケット5を生成する。認証子は認証チケットの改ざん防止と発行者の証明とを目的として付加されるもので、メッセージ認証コードやデジタル署名などが使用できる。

【0037】クライアント手段1と認可サーバ手段3との利用認可手順においては、クライアント手段1が秘密情報4に不可逆演算 $f$ を $n-k$ 回（ $k$ は認証チケットの利用認可手順での使用回数）行なった結果を提示情報6として用いる。不可逆演算 $f$ が充分安全な不可逆性と結果の長さ及びランダム性を持っている限り、この提示情報6は秘密情報4を知らない第三者には計算することができないため、この提示情報6により秘密情報4を知る正当なユーザであることが示される。また、過去にさかのぼるほど提示情報における不可逆演算 $f$ の回数が多く行なわれているため、この提示情報6から次の提示情報を計算することもできないので、暗号化の必要もない。

【0038】クライアント手段1は、この提示情報6を、保持していた認証チケット7とともに認可サーバ手段3に送り、これに対し認可サーバ手段3は、認証チケット7が含む認証子の検証と、提示情報6に不可逆演算 $f$ を $k$ 回行なった結果が認証チケット7が含む照合情報に一致することの確認とを行なって、正当と認めれば認可通知8を送り返す。

【0039】この方法により、クライアント手段1は秘密情報4を認可サーバ手段3を含めた第三者に明かすことなく、 $n$ 回まで認証チケット7を使用して利用認可を得ることができる。

【0040】このように、本実施の形態の認証システムは、有効回数が $n$ （ $n$ は正整数）である認証チケットを保持し、これを示して利用認可を求めるクライアント手段と、これを受けて提示情報を要求し前記認証チケットと照合して利用認可する認可サーバ手段とを具備している。

【0041】前記認証チケットには、照合情報の他に、チケット識別子、有効回数、発行日時、サーバ識別子な

どの情報を含めることができ、これに認証子が付与される。照合情報は、認証チケットの発行者とクライアント手段とが共有する秘密情報に所定の不可逆演算を $n$ 回施した情報である。また、前記提示情報は、認証チケットの使用回数が $k$ （ $k$ は $n$ 以下の正整数）であるとき、前記秘密情報に所定の不可逆演算を $n-k$ 回施した情報である。

【0042】こうした構成により、クライアント側での暗号処理を必要とせず、認証チケットの使用回数を容易に管理して二重使用を排除することができる、シングルサインオン型の認証方法及び認証システムが得られる。

【0043】（第2の実施の形態）第2の実施形態の認証システムでは、クライアント手段が、認証サーバ手段22に対して認証提示情報を示して認証チケットを要求する。

【0044】この認証システムは、図2に示すように、ユーザインタフェースを持つクライアント手段11と、ユーザ認証を行なう認証サーバ手段12と、クライアント手段11のアクセス権限を判断して利用認可を行なう認可サーバ手段3とから成り、クライアント手段11と認証サーバ手段12及び認可サーバ手段3との間は有線または無線通信ネットワークにより接続されている。この認可サーバ手段3は第1の実施形態（図1）と同一であり、また、認証サーバ手段12からクライアント手段11に送り返される認証チケット、クライアント手段11が認可サーバ手段3に送信する提示情報及び認可チケット、さらに認可サーバ手段3からクライアント手段11に送り返される認可通知8についても、第1の実施形態（図1）と同一である。

【0045】この認証システムのクライアント手段11と認証サーバ手段12とは、ユーザインタフェースを介して入力されたパスワード $PW$ と認証サーバ手段12より得た乱数 $R$ との連結に不可逆演算 $f$ を1回行なった結果を秘密情報14として共有する。不可逆演算 $f$ が充分安全な不可逆性と結果の長さ及びランダム性を持っている限り、この秘密情報14はパスワード $PW$ を知らない第三者には計算することができない。

【0046】クライアント手段11と認証サーバ手段12とのユーザ認証手順においては、認証サーバ手段12が乱数を生成し、これを示してクライアント手段11に認証提示情報を要求する。クライアント手段11は、パスワード $PW$ と認証サーバ手段12より得た乱数 $R$ との連結に不可逆演算 $f$ を1回行なって秘密情報14を算出し、この秘密情報14にさらに不可逆演算 $f$ を $n$ 回（通算 $n+1$ 回、 $n$ は認証チケットの有効回数）行なった結果を認証提示情報13として認証サーバ手段12に送る。

【0047】これに対し、認証サーバ手段12は、認証提示情報13から秘密情報14が一致していることを確認すると、秘密情報14に不可逆演算 $f$ を $n$ 回行なった結果を照合情報として、これに認証子を付加した認証チケット5

を送り返す。クライアント手段11は、これを利用認可手順で用いるために保持する。認証子は認証チケットの改ざん防止と発行者の証明を目的として付加されるもので、メッセージ認証コードやデジタル署名などが使用できる。

【0048】また、クライアント手段11と認可サーバ手段3との利用認可手順においては、クライアント手段11が秘密情報14に不可逆演算 $f$ を $n-k$ 回（ $k$ は認証チケットの利用認可手順での使用回数）行なった結果を提示情報6として用いる。不可逆演算 $f$ が充分安全な不可逆性と結果の長さ及びランダム性を持っている限り、この提示情報6は秘密情報14を知らない第三者には計算することができないため、この提示情報6により秘密情報14を知る正当なユーザであることが示される。また、過去にさかのぼるほど提示情報における不可逆演算 $f$ の回数が多く行なわれているため、この提示情報6から次の提示情報を計算することもできないので、暗号化の必要もない。

【0049】クライアント手段11は、この提示情報6を、保持していた認証チケット7とともに認可サーバ手段3に送り、これに対し認可サーバ手段3は認証チケット7が含む認証子の検証と、提示情報6に不可逆演算 $f$ を $k$ 回行なった結果が認証チケット7が含む照合情報に一致することの確認とを行なって、正当と認めれば認可通知8を送り返す。

【0050】この方法により、クライアント手段11は秘密情報14やパスワードPWを認可サーバ手段3を含めた第三者に明かすことなく、 $n$ 回まで認証チケット7を使用して利用認可を得ることができる。

【0051】このように、本実施の形態の認証システムでは、認証サーバ手段が、ユーザ認証手順において乱数を生成し、これを示してクライアント手段に認証提示情報を要求する。このときの秘密情報として、ユーザ認証情報と乱数との連結に所定の不可逆演算を1回以上施したものを使用し、認証提示情報として、この秘密情報に所定の不可逆演算を $n$ 回施したものが提示される。

【0052】こうした構成により、第1の実施形態の効果に加えて、ユーザ認証手順においてもクライアント側での暗号処理が不要であり、また、認証提示情報の演算処理と提示情報の演算処理とが共通化できる、シングルサインオン型の認証方法及び認証システムが得られる。

【0053】（第3の実施の形態）第3の実施形態の認証システムでは、図3に示すように、クライアント手段21によって生成された認証用乱数が秘密情報24としてクライアント手段21と認証サーバ手段22との間で共有される。

【0054】このシステムでは、ユーザ認証手順において、認証サーバ手段22が乱数を生成し、これを示してクライアント手段21に認証提示情報を要求する。クライアント手段21は、パスワードPWと認証サーバ手段22より

得た乱数 $R$ との連結に不可逆演算 $f$ を1回行なった結果とクライアント手段21が秘密裏に生成した秘密情報24との排他的論理和結果を認証提示情報23として認証サーバ手段22に送る。図3において、記号「@」は排他的論理和（ $\text{EXOR}$ ）演算を示している。

【0055】これに対し、認証サーバ手段22は、認証提示情報23とパスワードPWと乱数 $R$ とから逆算して秘密情報25を求める。そして、この秘密情報25に不可逆演算 $f$ を $n$ 回行ない、その演算結果を照合情報とし、これに認証子を付加した認証チケット5をクライアント手段21に送り返す。クライアント手段21は、これを利用認可手順で用いるために保持する。

【0056】なお、もしユーザが不正な第三者で認証提示情報23が適当に作られたものだとすれば、クライアント手段21で認証チケット5を入手することができても、サーバが認証提示情報23からパスワードPWと乱数 $R$ とを用いて逆算した秘密情報25はクライアント手段21には分からない。そのため、後続の利用認可手順においてその不正なアクセスを排除することができる。

【0057】クライアント手段21と認可サーバ手段3との利用認可手順においては、クライアント手段21が秘密情報24に不可逆演算 $f$ を $n-k$ 回（ $k$ は認証チケットの利用認可手順での使用回数）行なった結果を提示情報6として用いる。不可逆演算 $f$ が充分安全な不可逆性と結果の長さ及びランダム性を持っている限り、この提示情報6は秘密情報24を知らない第三者には計算することができないため、この提示情報6により秘密情報24を知る正当なユーザであることが示される。また、過去にさかのぼるほど提示情報における不可逆演算 $f$ の回数が多く行なわれているため、この提示情報6から次の提示情報を計算することもできないので、暗号化の必要もない。

【0058】クライアント手段21は、この提示情報6を、保持していた認証チケット7とともに認可サーバ手段3に送り、これに対し認可サーバ手段3は認証チケット7が含む認証子の検証と、提示情報6に不可逆演算 $f$ を $k$ 回行なった結果が認証チケット7が含む照合情報に一致することの確認とを行なって、正当と認めれば認可通知8を送り返す。

【0059】この方法により、クライアント手段21は、秘密情報24やパスワードPWを認可サーバ手段3を含めた第三者に明かすことなく、 $n$ 回まで認証チケット7を使用して利用認可を得ることができる。

【0060】このように、本実施の形態の認証システムでは、認証サーバ手段は、ユーザ認証手順において乱数を生成し、これを示してクライアント手段に認証提示情報を要求する。認証提示情報は、ユーザ認証情報及び前記乱数との連結に所定の不可逆演算を1回以上施したものと、クライアント手段が生成した認証用乱数（秘密情報）との排他的論理和演算結果であり、この秘密情報は、認証サーバ手段により認証提示情報から逆算され

る。

【0061】こうした構成により、認証チケットが含む照合情報がユーザ認証情報と無関係となる。そのため認証チケットからユーザ認証情報が推測される可能性すらないより安全な、シングルサインオン型の認証方法及び認証システムが得られる。

【0062】（第4の実施の形態）第4の実施形態では、第2の実施形態の認証システムにおける具体的な通信手順とそれを実行する各手段のブロック構成について説明する。

【0063】図4は、このシステムでのプロトコルを示すプロトコルシーケンス図である。図4において、31はユーザインタフェースを持つクライアント手段、32はユーザ認証を行なう認証サーバ手段、33はアクセス権限を判断して利用認可を行なう認可サーバ手段を示し、記号「S(K|~)」は鍵Kを用いた認証子添付関数を示している。

【0064】クライアント手段31と認証サーバ手段32とのユーザ認証手順においては、まず、クライアント手段31が、ユーザインタフェースを介して入力されたユーザ識別子UIDとサーバ識別子SIDとをともなった認証要求Authenticate Request301を認証サーバ手段32に送る。この時、認証要求Authenticate Request301が認証チケットの有効回数nをとともなうものとしてもよい。そうでない場合には、認証サーバが固定的に有効回数nを定めるものとすればよい。

【0065】これに対して、認証サーバ手段32は、毎回異なるように生成された乱数ROをとともなった認証チャレンジChallenge302を送り返す。これを受けたクライアント手段31は、ユーザインタフェースを介して入力されたパスワードPWと乱数ROとの連結に対してn+1段のハッシュ演算Hを施した結果をとともなった認証チャレンジ応答Response303を送り返し、これに対し認証サーバ手段32は、チャレンジ応答Response303におけるn+1段ハッシュ演算結果と自ら行なったn+1段ハッシュ演算結果とを比較検証して一致すれば正当と認め、新たに生成したチケット識別子TIDとn+1段ハッシュ演算結果とタイムスタンプTSOとサーバ識別子SIDと認証サーバ32自身を示す発行者識別子IIDとをともない認証子が付加された認証チケットTicket304を送り返す。クライアント手段31は、これを利用認可手順で用いるために保持する。

【0066】また、クライアント手段31と認可サーバ手段33との利用認可手順においては、クライアント手段31が認可要求Authorize Request及び認証チケットTicket305を認可サーバ手段33に送る。この時、認可要求Authorize Requestがユーザ識別子UIDをとともなうものとしてもよい。これに対して、認可サーバ手段33は、この認証チケットの使用回数に基づく値kをとともなった認可チャレンジChallenge306を送り返す。これを受けたクライ

アント手段31は、パスワードPWと乱数ROとの連結に対してn-k+1段のハッシュ演算Hを施した結果をとともなった認可チャレンジ応答Response307を送り返す。

【0067】このハッシュ演算Hが充分安全な一方向性と結果の長さ及びランダム性を持っている限り、このハッシュ演算結果はパスワードPW及び乱数ROを知らない第三者には計算することができないため、このハッシュ演算結果によりパスワードPWを知る正当なユーザであることが示される。また、過去にさかのぼるほどハッシュ演算Hの段数が多く行なわれているため、このハッシュ演算結果から次のハッシュ演算結果を計算することもできないので、暗号化の必要もない。このようなハッシュ演算Hとしては、例えばMD5やSHAなどのアルゴリズムを使用することができる。

【0068】これに対して、認可サーバ手段32は、認可チャレンジ応答Response307におけるn-k+1段ハッシュ演算結果にさらにk段のハッシュ演算を施した結果と認証チケットTicketにおけるn+1段ハッシュ演算結果とを比較検証し、一致すれば正当と認めて認可通知Result308を送り返す。この時、認可通知308が利用認可によりアクセスが許可された情報Infoを同時にともなうものとしてもよい。

【0069】以上のようなプロトコルシーケンスにより、クライアント手段31はパスワードPWを認可サーバ手段33を含めた第三者に明かすことなく、n回まで認証チケット304を使用して利用認可を得ることができる。

【0070】このようなプロトコルシーケンスを持つ認証システムの構成について図5の機能ブロック図を参照しながら説明する。

【0071】図5において、31はユーザインタフェースを持つクライアント手段、32はユーザ認証を行なう認証サーバ手段、33はアクセス権限を判断して利用認可を行なう認可サーバ手段である。

【0072】クライアント手段31は、データの送受信を行なう第1の送受信手段311と、ユーザからの入力を得る入力手段312と、2つの入力を連結してハッシュ演算Hを行なうハッシュ手段313と、受信した認証チケットを保持するチケット保持手段314と、認証チケットの保持状態に応じて処理を選択する処理選択手段315と、ハッシュ演算結果を秘密裏に記憶する機密記憶手段316と、与えられた段数または与えられた2つの数値の差の段数のハッシュ演算を行なう多段ハッシュ手段317とを備えている。

【0073】第1の送受信手段311は、通信ネットワークの種類に応じて例えばLANカード等のLANインタフェース装置、ターミナルアダプタ等のISDNインタフェース装置、モデム等の電話インタフェース装置、携帯データ通信カードやPIAFSカード等の無線インタフェース装置、IrDAモジュール等の赤外線インタフェース装置などで構成され、通信相手に応じてこれらの

いくつかを使い分ける構成としてもよい。入力手段312は、例えばキーボード、テンキー等の文字入力装置、マウス、トラックボール、ペンタブレット等のポインティングデバイスや選択ボタンやダイヤルと表示画面との組合せ、あるいはタッチパネルなどで構成される。ハッシュ手段313は、例えば論理回路とハッシュ演算Hのアルゴリズムを組み込んだ演算回路とを組み合わせて構成される。チケット保持手段314は、例えばメモリ回路が使用される。処理選択手段315は、例えば論理回路が使用できる。機密記憶手段316は、例えばICカードのような耐タンパ性を持ったメモリデバイスによって構成される。多段ハッシュ手段317は、例えばハッシュ演算Hのアルゴリズムを組み込んだ演算回路に出力をフィードバックする結線や段数をカウントするカウンタや数値の差を求める演算回路などを追加して構成される。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読み取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【0074】また、認証サーバ手段32は、データの送受信を行なう第2の送受信手段321と、現在時刻を計時する認証計時手段322と、パスワード等のユーザ認証情報を蓄積する認証情報蓄積手段323と、ユーザ認証処理毎に乱数を生成する乱数生成手段324と、与えられたよりも1多い段数のハッシュ演算Hを行なう第2の多段ハッシュ手段325と、2つの多段ハッシュ値を比較照合する認証照合手段326と、認証チケット発行毎にユニークなチケット識別子を生成するチケット識別子生成手段327と、認証チケットに対する認証子を生成して付加する認証子付加手段328とを備えている。

【0075】第2の送受信手段321は、通信ネットワークの種類に応じて例えばLANカード等のLANインタフェース装置、ターミナルアダプタ等のISDNインタフェース装置、モデム等の電話インタフェース装置、携帯データ通信カードやPIAFSカード等の無線インタフェース装置、IrDAモジュール等の赤外線インタフェース装置などで構成される。認証計時手段322は、例えばタイマカウンタが使用される。認証情報蓄積手段323は、大容量のメモリデバイスで構成され、耐タンパ性を持ったメモリデバイスであればなお良い。乱数生成手段324は、例えば乱数生成アルゴリズムを組み込んだ演算回路、あるいは電磁的ノイズをデータ化する変換装置などで構成される。第2の多段ハッシュ手段325は、例えばハッシュ演算Hのアルゴリズムを組み込んだ演算回路に出力をフィードバックする結線や段数をカウントするカウンタなどを追加して構成される。認証照合手段326は、例えば比較回路で構成される。チケット識別子生成手段327は、例えば十分なビット長を持ったカウンタ

回路で構成される。認証子付加手段328は、認証子生成アルゴリズムを組み込んだ演算回路及びメモリ回路で構成される。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読み取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【0076】また、認可サーバ手段33は、データの送受信を行なう第3の送受信手段331と、現在時刻を計時する認可計時手段332と、認証チケットに付加された認証子を検証する認証子検証手段333と、認証チケットの有効性判定を行なうチケット有効判定手段334と、認証チケットのチケット識別子と有効回数と残り利用可能回数を管理するチケット利用管理手段335と、与えられた段数のハッシュ演算Hを行なう第3の多段ハッシュ手段336と、2つの多段ハッシュ値を比較照合する認可照合手段337とを備えている。

【0077】第3の送受信手段331は、通信ネットワークの種類に応じて例えばLANカード等のLANインタフェース装置、ターミナルアダプタ等のISDNインタフェース装置、モデム等の電話インタフェース装置、携帯データ通信カードやPIAFSカード等の無線インタフェース装置、IrDAモジュール等の赤外線インタフェース装置などで構成される。認可計時手段332は、例えばタイマカウンタが使用される。認証子検証手段333は、認証子検証アルゴリズムを組み込んだ演算回路及びメモリ回路で構成される。チケット有効判定手段334は、例えば比較回路の組合せにより構成される。チケット利用管理手段335は、利用回数を計算する演算回路と大容量のメモリデバイスとの組合せにより構成される。第3の多段ハッシュ手段336は、例えば第2の多段ハッシュ手段325と同様の演算回路でカウンタのプリセット値を改めもので構成される。認可照合手段337は、例えば比較回路で構成される。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読み取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【0078】以上のように構成された認証方法及び認証システムにおいて、以下その動作について図6を参照しながら説明する。ここでは、認証要求Authenticate Request301が認証チケット有効回数 $n$ をとともう場合について説明する。

【0079】まず、クライアント手段31において、ユーザ自身を示すユーザ識別子UIDと認証サーバ手段32にあらかじめ登録されたユーザ認証用のパスワードPWと利用認可を得る対象のサーバ識別子SIDと認証チケットの有効回数 $n$ とがユーザ入力300として入力手段312に



入力される（ST3101、ST3104）。入力手段312は、ユーザ入力300を一時保持するとともにサーバ識別子3101を取出してチケット保持手段314に送る。チケット保持手段314は、サーバ識別子3101に対応する認証チケットデータを検索して（ST3102）、検索結果通知3102を処理選択手段315に送る。処理選択手段315は、検索結果通知3102が無しを示す場合には、ユーザ認証処理起動通知3103を前記入力手段312及び多段ハッシュ手段317に送り、有りを示す場合には（ST3103）、利用認可手順起動通知3104を前記チケット保持手段314と機密記憶手段316と多段ハッシュ手段317とに送る。

【0080】前記入力手段312は、ユーザ認証起動通知3103が与えられると、一時保持したユーザ入力300から取出した、ユーザ識別子とサーバ識別子と有効回数の組3105を第1の送受信手段311を介して認証要求Authenticate Request301として認証サーバ手段32に送り（ST3105）、有効回数3106を多段ハッシュ手段317に送り、パスワード3107をハッシュ手段313に送る。

【0081】認証サーバ手段32においては、認証要求Authenticate Request301は第2の送受信手段321で受信され、取出されたユーザ識別子3201が認証情報蓄積手段323に送られ、有効回数3202が第2の多段ハッシュ手段325及び認証子付加手段328に送られ、サーバ識別子3203が認証子付加手段328に送られる（ST3201）。認証情報蓄積手段323は、ユーザ識別子3201に対応するパスワードを検索して（ST3202）、有りの場合には（ST3203）、パスワード3204を第2の多段ハッシュ手段325に送り、検索結果通知3205を乱数生成手段324及び第2の多段ハッシュ手段325に送る。

【0082】乱数生成手段324は、検索結果通知3205が有りを示す場合に、データ攪乱用のチャレンジ乱数3206を新たにランダムに生成して第2の多段ハッシュ手段325に送るとともに、第2の送受信手段321を介して認証チャレンジChallenge302としてクライアント手段31に送る（ST3204）。第2の多段ハッシュ手段325は、検索結果通知3205が有りを示す場合に、パスワード3204とチャレンジ乱数3206との連結に対し有効回数3202より1多い段数のハッシュ演算Hを行なって、結果の多段ハッシュ値3207を認証照合手段326に送る（ST3205）。

【0083】これに対してクライアント手段31においては、認証チャレンジChallenge302は第1の送受信手段311で受信され、チャレンジ乱数3108が取り出されてハッシュ手段313に送られる（ST3106）。ハッシュ手段313はパスワード3107とチャレンジ乱数3108との連結に対するハッシュ演算Hを行なって（ST3107）、結果のハッシュ値3109を機密記憶手段316及び多段ハッシュ手段317に送る。機密記憶手段316はハッシュ値3109を秘密裏に記憶して所定のアクセスのみ、すなわちユー

ザ認証手順における追加更新及び利用認可手順における参照のみ許容する（ST3108）。多段ハッシュ手段317は、ユーザ認証手順起動通知3103が与えられている時、ハッシュ値3109に有効回数3106に相当する段数のハッシュ演算Hを行なって（ST3109）、結果の多段ハッシュ値3114を、第1の送受信手段311を介して認証チャレンジ応答Response303として認証サーバ手段32に送る（ST3110）。

【0084】これに対して認証サーバ手段32においては、認証チャレンジ応答Response303は第2の送受信手段321で受信され、多段ハッシュ値3208が取出されて認証照合手段326に送られる（ST3206）。認証照合手段326は、多段ハッシュ値3207と多段ハッシュ値3208との一致判定を行ない（ST3207）、照合結果3209をチケット識別子生成手段327に送るとともに多段ハッシュ値3208をそのまま多段ハッシュ値3210として認証子付加手段328に送る。チケット識別子生成手段327は、照合結果327が一致を示す場合に、有効なチケット識別子3212を生成して認証子付加手段328に送る（ST3208）。

【0085】認証計時手段322は、現在時刻を計時しており、現在時刻に基づくタイムスタンプ3211を認証子付加手段328に供給している。認証子付加手段328は、チケット識別子3212と多段ハッシュ値3210と有効回数3202とタイムスタンプ3211とサーバ識別子3203と認証サーバ32自身を示す発行者識別子とを連結し、これに対して認証子を生成して付加して認証チケットデータ3213とし（ST3209）、第2の送受信手段321を介して認証チケットTicket304としてクライアント手段31に送る（ST3210）。

【0086】これに対してクライアント手段31においては、認証チケットTicket304は第1の送受信手段311で受信され、認証チケットデータ3110が取出されて前記チケット保持手段314に送られる（ST3111）。前記チケット保持手段314は認証チケットデータ3110をサーバ識別子3101と対応づけて保持し（ST3112）、利用認可手順起動通知3104が与えられた場合に、認証チケットデータ3111を第1の送受信手段311を介して認証チケットTicket305として認可要求Authorize Requestとともに認可サーバ手段33に送る（ST3113）とともに、認証チケットデータから有効回数3112を取出して多段ハッシュ手段317に送る。

【0087】これに対して認可サーバ手段33においては、認証チケットTicket305をともなった認可要求Authorize Requestは第3の送受信手段331で受信され、認証チケットデータ3301が取出されて認証子検証手段333に送られる（ST3301）。認証子検証手段333は、認証チケットデータ3301の認証子と認証子以外のデータ部との整合性を検証して検証結果3304をチケット有効判定手段334に送るとともに（ST3304）、データ部か

らタイムスタンプ3302とサーバ識別子3303とを取出してチケット有効判定手段334に、チケット識別子3305と多段ハッシュ値3306と有効回数3307と発行者識別子3308とを取出してチケット利用管理手段335に、それぞれ送る。

【0088】認可計時手段332は、現在時刻を計時しており、現在時刻に基づくタイムスタンプ3309をチケット有効判定手段334に供給している。チケット有効判定手段334は、検証結果3304が誤りなしを示す場合に（ST3305）、サーバ識別子3303と内部に保持した自サーバ識別子との一致判定を行なうとともに（ST3302、ST3303）、タイムスタンプ3302と現在時刻に基づくタイムスタンプ3309との差が所定の有効期限の範囲内であることをチェックして（ST3306、ST3307）、いずれも真である場合にチケット有効通知3310をチケット利用管理手段335に送る。この有効期限は、短く設定するとセキュリティは向上するがユーザ利便性は低下し、長く設定するとユーザ利便性は向上するがセキュリティは低下するため、これらのバランスを勘案して定めるべきである。例えば厳重なセキュリティまでは要求されていない業務用システムに適用するならば1日の勤務時間をカバーできる8時間なり12時間なりにすればよい。ただし、最短でもクライアント〜サーバ間の通信時間及び各計時手段の間の時刻誤差をカバーできる必要がある。

【0089】このとき、チケット利用管理手段335はチケットリストを管理しており、チケット有効通知3310が与えられた場合に、チケット識別子3305を用いてチケットリスト中を検索して既に登録されているかを調べる（ST3308）。該当するものが無ければチケット識別子3305と有効回数3307と残り利用可能回数とを示す値としての有効回数3307の組をチケットリストに追加し記憶する（ST3309、ST3310）。この時、多段ハッシュ値3306と発行者識別子3308をあわせて記憶してもよい。この追加した組、あるいは検索で該当するものがあつた場合は当該の組みに対し、チケット利用管理手段335は残り利用可能回数を1減じ、有効回数と残り利用可能回数との差が示す利用回数3311を求め（ST3311）、これを第3の送受信手段331を介して認可チャレンジ（Challenge306としてクライアント手段31に送るとともに（ST3312）、第3の多段ハッシュ手段336にも送る。また、多段ハッシュ値3306をそのまま多段ハッシュ値3312として認可照会手段337に送る。

【0090】これに対してクライアント手段31においては、認可チャレンジ（Challenge306は第1の送受信手段31で受信され、利用回数3115が取出されて多段ハッシュ手段317に送られる（ST3114）。多段ハッシュ手段317は、利用認可手順起動通知3104が与えられている場合に、前記機密記憶手段316よりハッシュ値3113を得て（ST3115）、ハッシュ値3113に有効回数3112と

利用回数3115との差に相当する段数のハッシュ演算Hを行なって（ST3116）、結果の多段ハッシュ値3116を、第1の送受信手段311を介して認可チャレンジ応答Response307として認可サーバ手段33に送る（ST3117）。

【0091】ハッシュ演算Hが充分安全な方向性と結果の長さ及びランダム性を持っている限り、この多段ハッシュ値3116はパスワードPW及び乱数ROを知らない第三者には計算することができないため、この多段ハッシュ値3116によりパスワードPWを知る正当なユーザであることが示される。また、過去にさかのぼるほど多段ハッシュ値におけるハッシュ演算Hの段数が多く行なわれているため、この多段ハッシュ値3116から次の多段ハッシュ値を計算することもできないので、暗号化の必要もない。なお、ハッシュ演算は一般に暗号演算よりも100倍以上高速であるとされ、適切な段数であれば暗号を用いた場合よりも高速に処理が行なえる。

【0092】これに対して認可サーバ手段33においては、認可チャレンジ応答Response307は第3の受信手段331で受信され、多段ハッシュ値3313が取出されて第3の多段ハッシュ手段336に送られる（ST3313）。第3の多段ハッシュ手段336は、多段ハッシュ値3313に利用回数3311に相当する段数のハッシュ演算Hを行なって、結果の二次多段ハッシュ値3314を認可照会手段337に送る（ST3314）。認可照会手段337は、多段ハッシュ値3312と二次多段ハッシュ値3314との一致判定を行ない（ST3315、ST3316）、真であるならば認可通知3315を、第3の送受信手段331を介して認可通知Result308としてクライアント手段31に送り（ST3317）、クライアント手段31において受信される（ST3118）。この方法により、クライアント手段31はパスワードPWを認可サーバ手段33を含めた第三者に明かすことなく、n回まで認証チケット305を使用して利用認可を得ることができる。

【0093】なお、以上の説明ではクライアント手段31において利用認可手順のたびに多段ハッシュ値を計算する構成としたが、認証チケットの取得時にすべての段数の多段ハッシュ値を事前計算して機密記憶手段316に記憶する構成としても良い。その場合、機密記憶手段316としてより大容量の耐タンパ性メモリデバイスを用いる必要があるものの、利用認可手順ごとの処理時間をより短くすることができる。

【0094】次に、図5に示した第4の実施形態の認証システムにおいて、認証子としてメッセージ認証コードを用いた場合の認証子付加手段328及び認証子検証手段333の詳細な構成例及び動作について、図7及び図8を参照して説明する。

【0095】認証子付加手段328は、図7に示すように、認証サーバ自身を示す識別子が記憶された自識別子記憶手段328Aと、データを連結するデータ連結手段328B

と、ハッシュ演算  $h$  を行なう連結データハッシュ手段 328C と、認証サーバ手段 31 と認可サーバ手段 32 とが共通の秘密として持つサーバ共通鍵を記憶するサーバ共通鍵記憶手段 328D と、共通鍵方式の暗号処理を行なう共通鍵方式暗号手段 328E と、認証子をデータに連結する認証子連結手段 328F とを具備している。

【0096】この自識別子記憶手段 328A は、例えばメモリで構成される。データ連結手段 328B は、例えば論理回路で構成できる。連結データハッシュ手段 328C は、例えばハッシュ演算  $h$  のアルゴリズムを組み込んだ演算回路で構成される。ここでハッシュ演算  $h$  は、ハッシュ演算  $H$  と同じであっても異なっても良い。サーバ共通鍵記憶手段 328D は、例えばメモリで構成され、耐タンパ性を持ったメモリデバイスであればなお良い。共通鍵方式暗号手段 328E は、例えば暗号アルゴリズムを組み込んだ演算回路または暗号処理専用プロセッサで構成される。ここで暗号アルゴリズムとしては、例えば DES や トリプル DES などが使用できる。認証子連結手段 328F は、例えば論理回路で構成される。

【0097】また、認証子検証手段 333 は、図 8 に示すように、認証子をデータから分離する認証子分離手段 333A と、ハッシュ演算  $h$  を行なう第 2 の連結データハッシュ手段 333B と、認証サーバ手段 31 と認可サーバ手段 32 とが共通の秘密として持つサーバ共通鍵を記憶する第 2 のサーバ共通鍵記憶手段 333C と、共通鍵方式の暗号処理を行なう第 2 の共通鍵方式暗号手段 333D と、データ部を分割分離するデータ分離手段 333E と、発行者識別子を照合する発行者識別子照合手段 333F と、メッセージ認証コードを比較検証する比較手段 333G とを具備している。

【0098】この認証子分離手段 333A は、例えば論理回路で構成される。第 2 の連結データハッシュ手段 333B、第 2 のサーバ共通鍵記憶手段 333C 及び第 2 の共通鍵方式暗号手段 333D は、それぞれ図 7 における 328C、328D、328E と同じように構成される。データ分離手段 333E は、例えば論理回路で構成される。発行者識別子照合手段 333F は、例えばメモリ回路及び比較回路で構成される。比較手段 333G は、例えば比較回路の組合せにより構成される。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【0099】以上のように構成された認証子付加手段 328 及び認証子検証手段 333 の動作について説明する。認証子付加手段 328 では、まず、自識別子記憶手段 328A からデータ連結手段 328B に認証サーバ自身を示す識別子が発行者識別子 328a として供給されている。データ連結手段 328B は、第 2 の送受信手段 321 より得た有効回数 3202 及びサーバ識別子 3203 と、認証照合手段 326 より得た多段

ハッシュ値 3210 と、認証計時手段 322 より得たタイムスタンプ 3211 と、チケット識別子生成手段 327 より得たチケット識別子 3212 と、自識別子記憶手段 328A より得た発行者識別子 328a とを定められた順序で並べて連結し、データ部 328b として連結データハッシュ手段 328C 及び認証子連結手段 328F に送る。

【0100】連結データハッシュ手段 328C は、データ部 328b に対するハッシュ演算  $h$  を行なうと、結果のハッシュ値 328c を共通鍵方式暗号手段 328E に送る。共通鍵方式暗号手段 328E は、サーバ共通鍵記憶手段 328D からサーバ共通鍵 328d を得て、これを暗号鍵に用いてハッシュ値 328c を暗号化して、メッセージ認証コード 328e として認証子連結手段 328F に送る。認証子連結手段 328F は、データ部 328b にメッセージ認証コード 328e を連結して、認証チケットデータ 3213 を出力する。

【0101】また、認証子検証手段 333 では、まず、認証チケットデータ 3301 が認証子分離手段 333A に入力され、メッセージ認証コード 333a とデータ部 333b とに分離され、メッセージ認証コード 333a は比較手段 333G に、データ部 333b は第 2 の連結データハッシュ手段 333B 及びデータ分離手段 333E にそれぞれ送られる。第 2 の連結データハッシュ手段 333B は、データ部 333b に対するハッシュ演算  $h$  を行なうと、結果のハッシュ値 333c を第 2 の共通鍵方式暗号手段 333D に送る。第 2 の共通鍵方式暗号手段 333D は、第 2 のサーバ共通鍵記憶手段 333C からサーバ共通鍵 333d を得て、これを暗号鍵に用いてハッシュ値 333c を暗号化して、比較用メッセージ認証コード 333e として比較手段 333G に送る。データ分離手段 333E は、データ部 333b をタイムスタンプ 3302 とサーバ識別子 3303 とチケット識別子 3305 と多段ハッシュ値 3306 と有効回数 3307 と発行者識別子 3308 とに分離して出力するとともに、発行者識別子 3308 については発行者識別子照合手段 333F にも送る。発行者識別子照合手段 333F は、発行者識別子 3308 が認証サーバ 32 の識別子かどうかを照合し、照合結果 333f を比較手段 333G に送る。比較手段 333G は、照合結果 333f が一致を示すか、メッセージ認証コード 333a と比較用メッセージ認証コード 333e とが一致するかをもとに検証結果 3304 を出力する。検証結果 3304 が誤りなしを示すのは、いずれも一致した場合である。

【0102】次に、図 5 の第 4 の実施形態の認証システムにおいて、認証子としてデジタル署名を用いた場合の認証子付加手段 328 及び認証子検証手段 333 の構成及び動作について、図 9 及び図 10 を参照して説明する。図 9 において図 7 と異なるのは、サーバ共通鍵記憶手段 328D 及び共通鍵方式暗号手段 328E の代わりに、認証サーバ 32 自身の公開鍵方式暗号秘密鍵を記憶する自秘密鍵記憶手段 328G 及び公開鍵方式の暗号処理を行なう公開鍵方式暗号手段 328H を設けた点にある。自秘密鍵記憶手段 328G としては、例えばメモリが使用でき、耐タンパ性を持ったメモリデバイスであればなお良い。公開鍵方式暗号手段

328Hとしては、例えば暗号アルゴリズムを組み込んだ演算回路または暗号処理専用プロセッサが使用できる。ここで暗号アルゴリズムとしては、例えばRSAや楕円曲線暗号などが使用できる。

【0103】また、図10において図8と異なるのは、第2のサーバ共通鍵記憶手段333C、第2の共通鍵方式暗号手段333D及び発行者識別子照合手段333Fの代わりに、認証サーバ手段31の公開鍵をサーバ識別子と対応づけて1つ以上蓄積するサーバ公開鍵蓄積手段333H及び公開鍵方式暗号の復号処理を行なう公開鍵方式復号手段333Jを設け、これらの間の結線を改めた点にある。サーバ公開鍵蓄積手段333Hは、認証サーバ手段32のみならず認可サーバ手段33の公開鍵をも蓄積するものとしてもよい。サーバ公開鍵蓄積手段333Hとしては、例えばメモリ回路が使用でき、大容量のメモリデバイスであればなおよい。公開鍵方式復号手段333Jとしては、例えば復号アルゴリズムを組み込んだ演算回路または暗号処理専用プロセッサが使用できる。ここで復号アルゴリズムとしては、公開鍵方式暗号手段328Hにおける暗号アルゴリズムに対応する復号アルゴリズムを用いることは言うまでもない。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読み取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読み取り装置と組み合わせた構成により実現しても良い。

【0104】以上のように構成された認証子付加手段328及び認証子検証手段333の動作について説明する。認証子付加手段328では、自識別子記憶手段328A、データ連結手段328B、連結データハッシュ手段328Cの動作は図7の場合と同様であり、データ部328bが認証子連結手段328Fに、ハッシュ値328cが公開鍵方式暗号手段328Hに、それぞれ供給される。公開鍵方式暗号手段328Hは、自秘密鍵記憶手段328Gから自秘密鍵328fを得て、これを暗号鍵に用いてハッシュ値328cを暗号化して、デジタル署名328gとして認証子連結手段328Fに送る。認証子連結手段328Fは、データ部328bにデジタル署名328gを連結して、認証チケットデータ3213を出力する。

【0105】また、認証子検証手段333では、まず、認証チケットデータ3301が認証子分離手段333Aに入力され、デジタル署名333gとデータ部333bとに分離され、デジタル署名333gは公開鍵方式復号手段333Jに、データ部333bは第2の連結データハッシュ手段333B及びデータ分離手段333Eにそれぞれ送られる。第2の連結データハッシュ手段333Bは、データ部333bに対するハッシュ演算hを行なって、結果のハッシュ値333hを比較手段333Gに送る。データ分離手段333Eは、データ部333bをタイムスタンプ3302とサーバ識別子3303とチケット識別子3305と多段ハッシュ値3306と有効回数3307と発行者識別子3308とに分離して出力するとともに、発行者識別子3308につい

てはサーバ公開鍵蓄積手段333Hにも送る。サーバ公開鍵蓄積手段333Hは、発行者識別子3308が既知の認証サーバ31（または認可サーバ32）の識別子かどうか検索照合し、照合結果333iを比較手段333Gに送るとともに、発行者識別子3308に対応するサーバ公開鍵333jを公開鍵方式復号手段333Jに送る。

【0106】公開鍵方式復号手段333Jは、サーバ公開鍵333jを復号鍵に用いてデジタル署名333gを復号化して、比較用ハッシュ値333kとして比較手段333Gに送る。比較手段333Gは、照合結果333iが一致を示すか、ハッシュ値333hと比較用ハッシュ値333kとが一致するかをもとに検証結果3304を出力する。検証結果3304が誤りなしを示すのは、いずれも一致した場合である。

【0107】このように、認証システムがこの実施形態の構成を採ることにより、クライアント側が計算処理能力の低い装置であっても、実用的な処理時間で利用認可処理を行なうことが可能になる。

【0108】（第5の実施形態）第5の実施形態では、第3の実施形態の認証システムにおける具体的な通信手順とそれを実行する各手段のブロック構成について説明する。

【0109】図11は第5の実施形態における認証システムのプロトコルを示すプロトコルシーケンス図である。図11において図4と異なるのは、ユーザインタフェースを持つクライアント手段41とユーザ認証を行なう認証サーバ手段42とであって、認可サーバ手段33は変わらない。また、認証チャレンジ応答Response401がユーザインタフェースを介して入力されたパスワードPWと乱数R0との連結に対して1段のハッシュ演算Hを施した結果とクライアント手段41が秘密裏に生成した認証用乱数S0との排他的論理和結果（記号「@」は排他的論理和演算を示す）をとともなう点、認証チケットTicket402、403がともなうハッシュ演算結果が認証用乱数S0に対するn段のハッシュ演算結果である点、認可チャレンジ応答Response404がともなうハッシュ演算結果が認証用乱数S0に対するn-k段のハッシュ演算である点が異なる。

【0110】以上のようなプロトコルシーケンスにより、クライアント手段41はパスワードPWを認可サーバ手段33を含めた第三者に明かすことなく、n回まで認証チケット402を使用して利用認可を得ることができ、認証チケット402がパスワードPWに無関係の内容であるため、不正な第三者によるパスワードPWを盗むための攻撃対象にすらならず、より安全性が高い。

【0111】このようなプロトコルシーケンスを持つ認証システムの構成について図12の機能ブロック図を参照しながら説明する。

【0112】図12においても図5と異なるのは、ユーザインタフェースを持つクライアント手段41及びユーザ認証を行なう認証サーバ手段42であって、認可サーバ手

段33は変わらない。また、クライアント手段41において図5のクライアント手段31と異なるのは、ユーザ認証処理毎に乱数を生成する認証用乱数生成手段411、及びビット毎の排他的論理和演算を行なう第1の排他的論理和手段412を設け、一部の結線を改めた点にある。また、認証サーバ手段42において図5の認証サーバ手段32と異なるのは、第2の多段ハッシュ手段325、認証照合手段326の代わりに、ハッシュ演算Hを行なう第2のハッシュ手段421、ビット毎の排他的論理和演算を行なう第2の排他的論理和手段422、与えられた段数のハッシュ演算Hを行なう第2の多段ハッシュ手段423を設け、一部の結線を改めた点にある。認証用乱数生成手段411としては、例えば乱数生成アルゴリズムを組み込んだ演算回路、あるいは電磁的ノイズをデータ化する変換装置などが使用できる。第1、第2の排他的論理和手段412、422としては、例えば論理回路が使用できる。第2のハッシュ手段421としては、例えばハッシュ演算Hのアルゴリズムを組み込んだ演算回路が使用できる。第2の多段ハッシュ手段423としては、例えば421と同様の演算回路に出力をフィードバックする結線や段数をカウントするカウンタなどを追加して構成できる。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読み取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読み取り装置と組み合わせた構成により実現しても良い。

【0113】以上のように構成された認証システムの動作について図13を参照しながら説明する。ここでは、認証要求Authenticate Request301が認証チケット有効回数nをとともなう場合について説明する。

【0114】まず、クライアント手段41及び認証サーバ手段42において、第1、第2の送受信手段311、321、入力手段312、チケット保持手段314、処理選択手段315、認証情報蓄積手段323、乱数生成手段324の動作は図5、図6の場合と同様であり、認証要求Authenticate Request301及び認証チャレンジChallenge302が交換されて、クライアント手段41においてはユーザ認証処理起動通知4101または利用認可手順起動通知3104が、認証サーバ手段42においては有効回数4201とサーバ識別子3203とパスワード3204と検索結果通知4202とチャレンジ乱数3206とが得られる。ただし、ユーザ認証処理起動通知4101が前記入力手段312、認証用乱数生成手段411及び第1の排他的論理和手段412に送られる点、有効回数4201が第2の多段ハッシュ手段423及び認証子付加手段328に送られる点、検索結果通知4202が第2のハッシュ手段421、乱数生成手段324及びチケット識別子生成手段327に送られる点、チャレンジ乱数3206が第2のハッシュ手段421に送られるとともに第2の送受信手段321を介してクライアント手段41に送られる点が異なる。

【0115】次に、クライアント手段41において、認証

用乱数生成手段411は、ユーザ認証処理起動通知4101が与えられると、認証済み証明に用いられる認証用乱数4102を新たにランダムかつ秘密裏に生成して第1の排他的論理和手段412及び機密記憶手段316に送る(ST4101)。機密記憶手段316は、認証用乱数4102を秘密裏に記憶して所定のアクセスのみ、すなわちユーザ認証手順における追加更新及び利用認可手順における参照のみ許容する(ST4102)。第1の排他的論理和手段412は、ユーザ認証処理起動通知4101が与えられると、ハッシュ手段313より得たハッシュ値4103と認証用乱数4102との間でビット毎の排他的論理和演算を行ない、結果として得られた攪乱ハッシュ値4104を第1の送受信手段311を介して認証チャレンジ応答Response401として認証サーバ手段42に送る(ST4103、ST4104)。

【0116】これに対して認証サーバ手段42においては、認証チャレンジ応答Response401は第2の送受信手段321で受信され、攪乱ハッシュ値4204が取出されて第2の排他的論理和手段422に送られる(ST4202)。一方で第2のハッシュ手段421は、検索結果通知4202が有りを示す場合に、パスワード3204とチャレンジ乱数3206との連結に対しハッシュ演算Hを行なって、結果のハッシュ値4203を第2の排他的論理和手段422に供給している(ST4201)。第2の排他的論理和手段422は、第2のハッシュ手段421より得たハッシュ値4203と攪乱ハッシュ値4204との間でビット毎の排他的論理和演算を行ない、結果として得られた認証用乱数4205を第2の多段ハッシュ手段423に送る(ST4203)。第2の多段ハッシュ手段423は、認証用乱数4205に対し有効回数4201相当の段数のハッシュ演算Hを行なって、結果の多段ハッシュ値4206を認証子付加手段328に送る(ST4204)。

【0117】以下、チケット識別子生成手段327、認証計時手段322、認証子付加手段328の動作は図4、図5の場合と同様であるが、チケット識別子生成手段327が照合結果3209の代わりに検索結果通知4202を用いる点、認証子付加手段328が有効回数3202及び多段ハッシュ値3210の代わりに有効回数4201及び多段ハッシュ値4206を用いる点が異なり、認証チケットデータ3213とは異なる内容の認証チケットデータ4207が得られ(ST4205)、第2の送受信手段321を介して認証チケットTicket402としてクライアント手段41に送られる。

【0118】これに対してクライアント手段41においては、前記第1の送受信手段311、前記チケット保持手段314が図5、図6の場合と同様に動作し、利用認可手順起動通知3104が与えられた場合に、認証チケットTicket403が認可要求Authorize Requestとともに認可サーバ手段33に送られ、有効回数3112が多段ハッシュ手段317に供給される。

【0119】これに対する認可サーバ手段33の動作も図5、図6の場合と同様であり、認可チャレンジChallenge



e306が返される。

【0120】これに対してクライアント手段41においては、前記第1の送受信手段311、多段ハッシュ手段317が図5、図6の場合と同様に動作する。ただし、前記機密記憶手段316より得るのは認証用乱数4105であり（ST4105）、これに対して処理が行なわれる。すなわち、多段ハッシュ手段317が有効回数3112と利用回数3115との差に相当する段数のハッシュ演算Hを行なって（ST4106）、結果の多段ハッシュ値4106を第1の送受信手段311を介して認可チャレンジ応答Response404として認可サーバ手段33に送る（ST4107）。

【0121】これにより認可サーバ手段33が得る認可チャレンジ応答Response404がともなう多段ハッシュ値、認証チケットTicket403がともなう多段ハッシュ値は、図5、図6の場合とはハッシュ対象が異なるのみであり、前者と後者の演算関係は保たれている。従って、これに対する認可サーバ手段33の動作も図5、図6の場合と同様でよく、2つの多段ハッシュ値の関係をチェックして、正当と認めれば認可通知Result308が返され、クライアント手段41において受信される。この方法により、クライアント手段41はパスワードPWを認可サーバ手段33を含めた第三者に明かすことなく、かつパスワードPWとは無関係で安全性のより高い認証チケット402を使用してn回まで利用認可を得ることができる。

【0122】なお、以上の説明ではクライアント手段41において利用認可手順のたびに多段ハッシュ値を計算する構成としたが、認証チケットの取得時にすべての段数の多段ハッシュ値を事前計算して機密記憶手段316に記憶する構成としても良い。その場合、機密記憶手段316としてより大容量の耐タンパ性メモリデバイスを用いる必要があるものの、利用認可手順ごとの処理時間をより短くすることができる。

【0123】このように、認証システムがこの実施形態の構成を採ることにより、クライアント側が計算処理能力の低い装置であっても、実用的な処理時間で利用認可処理を行なうことが可能になる。また、認証チケットに含まれる照合情報がユーザ認証情報と無関係になるため、認証チケットからユーザ認証情報が推測される可能性が無くなり、より安全性の高い、シングルサインオン型の認証方法及び認証システムが得られる。

【0124】（第6の実施の形態）第6の実施形態の認証システムでは、認可サーバからクライアント手段に、認可通知とともに、利用回数が更新された認証チケットが送られる。

【0125】図14は、この認証システムのプロトコルを示すプロトコルシーケンス図である。図14において図4と異なるのは、クライアント手段51及び認可サーバ手段53であって、認証サーバ手段32は変わらない。また、認可サーバ53からクライアント手段51に、認可通知Result308とともに更新された認証チケットTicket501が

送られる点が異なる。

【0126】この認証チケットTicket501は、認証チケット305に比べて、次の点が相違している。

【0127】即ち、認証チケット305での $n+1$ 段ハッシュ演算結果が、 $n-k+1$ 段ハッシュ演算結果（ $k$ は利用回数）に置き換えられている。認証チケット305での有効回数 $n$ が、残り利用可能回数 $n-k$ に置き換えられている。タイムスタンプTS0が新たなタイムスタンプTS $k$ に置き換えられている。発行者識別子IIDが認可サーバ53自身を示すサーバ識別子に置き換えられている。さらに、新たな認証子が付加されている。

【0128】この方法により、クライアント手段51は、パスワードPWを認可サーバ手段53を含めた第三者に明かすことなく、 $n$ 回まで認証チケット304や更新された認証チケット501を使用して利用認可を得ることができる。また、認証チケットのタイムスタンプが毎回更新されるため有効期限をより短く設定できる。そのため、不正な第三者による攻撃対象になりうる期間が短くなり、より安全性が高い。また、認可サーバ手段53におけるハッシュ演算が1段で良いため、利用認可手順における応答時間が短縮できる。

【0129】このようなプロトコルシーケンスを持つ認証システムの構成について図15を参照しながら説明する。

【0130】図15において、図5と異なるのは、クライアント手段51及び認可サーバ手段53であり、認証サーバ手段32は変わらない。また、クライアント手段51において図5のクライアント手段31と異なるのは、チケット保持手段511が認可サーバ手段53からの認証チケットTicket501の認証チケットデータ5101も保持できるようにした点にある。また、認可サーバ手段53において図5の認可サーバ手段33と異なるのは、チケット利用管理手段531が残り利用可能回数をも出力するものとし、第3の多段ハッシュ手段336の代わりに1段のハッシュ演算Hを行なう第3のハッシュ手段532を設け、認証チケットに対する認証子を生成して付加する第2の認証子付加手段533を新たに設け、一部の結線を改めた点にある。

【0131】このチケット保持手段511としては、チケット保持手段314と同様の構成が結線を追加して使用できる。チケット利用管理手段531としては、チケット利用管理手段335と同様の構成が結線を追加して使用できる。第3のハッシュ手段532としては、例えばハッシュ演算Hのアルゴリズムを組み込んだ演算回路が使用できる。第2の認証子付加手段533としては、認証子付加手段328と同様の構成が使用できる。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読み取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読み取り装置と組み合わせた構成により実現しても良い。

【0132】以上のように構成された認証システムの動作について図16を参照しながら説明する。ここでは、認証要求Authenticate Request301が認証チケット有効回数nをとともう場合について説明する。

【0133】まず、クライアント手段51及び認証サーバ手段32における動作は図5、図6の場合と同様で、ユーザ認証手順が行なわれて最終的には、認証サーバ手段32よりクライアント手段51へ認証チケットTicket304が送られる。

【0134】これに対してクライアント手段51においては、第1の送受信手段311は図5、図6の場合と同様に動作し、チケット保持手段511は図5、図6の場合のチケット保持手段314と同様に動作し、認証チケットTicket305が認可要求Authorize Requestとともに認可サーバ手段53に送られるとともに、認証チケットデータから有効回数3112が取出され多段ハッシュ手段317に送られる。

【0135】これに対して認可サーバ手段53においては、第3の送受信手段331、認可計時手段332、認証子検証手段333及びチケット有効判定手段334は図5、図6の場合と同様に動作し、チケット識別子3305と多段ハッシュ値3306と有効回数3307と発行者識別子3308とチケット有効通知3310とをチケット利用管理手段531に供給する。チケット利用管理手段531は、図5、図6の場合のチケット利用管理手段335とほぼ同様に動作して、利用回数5301を第3の送受信手段331を介して認可チャレンジChallenge306としてクライアント手段51に送り、多段ハッシュ値3306をそのまま多段ハッシュ値5302として認可照合手段337に送るが、さらにチケット識別子と残り利用可能回数とサーバ識別子の組5303を出力して第2の認証子付加手段533に送る。

【0136】これに対するクライアント手段51の動作も図5、図6の場合と同様であり、認可チャレンジChallenge306に対して認可チャレンジ応答Response307が返される。

【0137】これに対して認可サーバ手段53においては、認可チャレンジ応答Response307は第3の送受信手段331で受信され、多段ハッシュ値5304が取出されて第3のハッシュ手段532及び第2の認証子付加手段533に送られる。第3のハッシュ手段532は、多段ハッシュ値5304にハッシュ演算Hを行なって、ハッシュの段数が1増えた二次多段ハッシュ値5305を認可照合手段337に送る(ST5301)。認可照合手段337は、多段ハッシュ値5302と二次多段ハッシュ値5305との一致判定を行ない(ST5302、ST3316)、照合結果5307を第2の認証子付加手段533に送る。

【0138】認可計時手段322は現在時刻を計時しており、現在時刻に基づくタイムスタンプ5306を第2の認証子付加手段533に供給している。第2の認証子付加手段533は、チケット識別子と残り利用可能回数とサーバ識別

子の組5303と多段ハッシュ値5304とタイムスタンプ5306と認可サーバ53自身を示す発行者識別子とを連結し、これに対して認証子を生成して付加して認証チケットデータ5308とし(ST5303)、第3の送受信手段331を介して認証チケットTicket501として認可通知Result308とともにクライアント手段51に送る(ST5304)。

【0139】これに対してクライアント手段51においては、認証チケットTicket501は第1の送受信手段311で受信され、認証チケットデータ5101として前記チケット保持手段511に送られ保持されて(ST5101、ST5102)、次の利用認可手順で使用される。

【0140】これによりクライアント手段51から認可サーバ手段53に送られる認証チケット305がともなう多段ハッシュ値は、その段数が利用認可ごとに1ずつ減って行くので、認可サーバ手段53ではハッシュ演算は1段のみ行なえば良く、応答時間が短縮できる。また、タイムスタンプが更新されるため有効期限をアクセスの間隔をカバーできる程度の短さ、例えば1時間に設定でき、ユーザ利便性は低下させずに安全性を高めることができる。この方法により、クライアント手段31はパスワードPWを認可サーバ手段53を含めた第三者に明かすことなく、安全性のより高い認証チケット305を使用してn回までより短い応答時間で利用認可を得ることができる。

【0141】なお、以上の説明ではクライアント手段51において利用認可手順のたびに多段ハッシュ値を計算する構成としたが、認証チケットの取得時にすべての段数の多段ハッシュ値を事前計算して機密記憶手段316に記憶する構成としても良い。その場合、機密記憶手段316としてより大容量の耐タンパ性メモリデバイスを用いる必要があるものの、利用認可手順ごとの処理時間をより短くすることができる。

【0142】このように、本実施の形態の認証システムでは、第三者による不正使用の可能性をより小さくでき、また、利用認可の応答時間を短縮することができる。

【0143】(第7の実施の形態) 第7の実施形態の認証システムは、認証チケットを複数の認可サーバに対して共通に用いることができる。

【0144】図17は、この認証システムのプロトコルを示すプロトコルシーケンス図である。図17において図4と異なるのは、クライアント手段61、認証サーバ手段62、認可サーバ手段63であって、さらに認証チケット管理手段64を追加している。また、認証チャレンジ応答Response303を受けた認証サーバ手段62が認証要求Authenticate Request301から取出したチケット識別子TIDとサーバ識別子SIDと有効回数nをとともなった認証チケット発行登録指示Registration601を認証チケット管理手段64へ送る点、認可要求Authorize Request602が利用回数kをとともなう点、認可要求Authorize Request602及び認証チケットTicket305を受けた認可サーバ手段6

3が認可要求Authorize Request602及び認証チケット305から取出したチケット識別子TIDとサーバ識別子SIDと利用回数kをとともなった認証チケット履歴更新指示Update603を認証チケット管理手段64へ送る点、これに対して必要に応じて認証チケット拒絶通知Reject606が返される点、認可チャレンジChallenge604が利用回数kの代わりに毎回異なるよう生成された乱数Rkをとともなう点、認可チャレンジ応答Response605がパスワードPWと乱数R0との連結に対して $n-k+1$ 段のハッシュ演算Hを施した結果にさらにRkとの排他的論理和演算を行なった結果をとともなう点異なる。

【0145】この方法により、クライアント手段61は、パスワードPWを認可サーバ手段63を含めた第三者に明かすことなく、n回まで認証チケット304を使用して利用認可を得ることができ、利用回数kをクライアント手段61から送って認可サーバ手段63とは独立した認証チケット管理手段64でチェックするため、認証チケット304を複数の認可サーバ手段63で共通に利用可能とすることができる。

【0146】このプロトコルシーケンスを持つ認証システムの構成について図18を参照しながら説明する。図18においても図5と異なるのは、クライアント手段61、認証サーバ手段62、及び認可サーバ手段63であって、さらに認証チケット管理手段64を追加している。また、クライアント手段61において図5のクライアント手段31と異なるのは、認証チケットを保持するとともにその利用回数kを管理するチケット保持管理手段611をチケット保持手段314の代わりに設け、ビット毎の排他的論理和演算を行なう第1の排他的論理和手段612を設け、一部の結線を改めた点にある。また、認証サーバ手段62において図5の認証サーバ手段32と異なるのは、認証チケット発行登録指示データを生成するチケット登録指示手段621を設け、一部の結線を改めた点にある。

【0147】また、認可サーバ手段63において図5の認可サーバ手段33と異なるのは、認証チケットのチケット識別子と有効回数と残り利用可能回数を受取って各部に供給するとともに認証チケット履歴更新指示データを生成するチケット更新指示手段631をチケット利用管理手段335の代わりに設け、利用認可処理毎に乱数を生成する第2の乱数生成手段632、ビット毎の排他的論理和演算を行なう第2の排他的論理和手段633を設け、一部の結線を改めた点にある。

【0148】このチケット保持管理手段611としては、チケット保持手段335と同様の構成に利用回数の計算を行なう加算回路を追加して構成される。第1、第2の排他的論理和手段612、633としては、例えば論理回路が使用できる。チケット登録指示手段621としては、例えば論理回路が使用できる。チケット更新指示手段631としては、例えば論理回路が使用できる。第2の乱数生成手段632としては、乱数生成手段324と同様の構成が使用で

きる。認証チケット管理手段64としては、各種通信インタフェース装置とデータの分割結合を行なう論理回路と利用回数を照合する演算回路及び比較回路と大容量のメモリデバイスとの組合せにより構成できる。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読み取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読み取り装置と組み合わせた構成により実現しても良い。

【0149】以上のように構成された認証システムの動作について図19を参照しながら説明する。ここでは、認証要求Authenticate Request301が認証チケット有効回数nをとともなう場合について説明する。

【0150】まず、ユーザ認証手順におけるクライアント手段61及び認証サーバ手段62における動作は図5、図6の場合とほぼ同様で、最終的には認証サーバ手段62よりクライアント手段61へ認証チケットTicket304が送られる。ただし、クライアント手段61においては、このときのチケット保持手段314の動作をチケット保持管理手段611が行なう。また認証サーバ手段62においては、認証要求Authenticate Request301から取出された有効回数6201は多段ハッシュ手段325及び認証子付加手段328のほかチケット登録指示手段621にも送られ、サーバ識別子6202は認証子付加手段328のほかチケット登録指示手段621にも送られ、チケット識別子生成手段327で生成されたチケット識別子6203は認証子付加手段328のほかチケット登録指示手段621にも送られる。

【0151】チケット登録指示手段621は、チケット識別子6203とサーバ識別子6202と有効回数6201とを連結して認証チケット発行登録指示データ6204を生成し、第2の送受信手段321を介して認証チケット発行登録指示Registration601として認証チケット管理手段64に送る(ST6201)。これを受けた認証チケット管理手段64はチケットリストを管理しており、認証チケット発行登録指示Registration601が与えられた場合に、チケット識別子を用いてチケットリスト中を検索して既に登録されているかを調べる。該当するものが無ければチケット識別子と有効回数と残り利用可能回数を示す値としての有効回数の組をチケットリストに追加し記憶する。

【0152】これに対してクライアント手段61においては、認証チケットTicket304は第1の送受信手段311で受信され、認証チケットデータ3110が取出されてチケット保持管理手段611に送られる。チケット保持管理手段611は認証チケットデータ3110をサーバ識別子3101と対応づけて保持し、認証チケットデータから取出した有効回数と残り利用可能回数として同時に管理し(ST6101)、利用認可手順起動通知6101が与えられた場合に、認証チケットデータ3111を第1の送受信手段311を介して認証チケットTicket305として、また、残り利用可能

回数を1減じたうえで認証チケットから取出した有効回数から引くことにより得た利用回数6102を（ST6102）第1の送受信手段311を介して認可要求Authorize Request602として、認可サーバ手段63に送り（ST6103）、さらに、認証チケットデータから取出した有効回数3112を多段ハッシュ手段317に送る。

【0153】これに対して認可サーバ手段63においては、認証チケットTicket305及び認可要求Authorize Request602は第3の送受信手段331で受信され、認証チケットデータ3301が取出されて認証子検証手段333に送られ、利用回数6301が取出されてチケット更新指示手段631に送られる（ST6301）。認可計時手段332、認証子検証手段333及びチケット有効判定手段334は図5、図6の場合とほぼ同様に動作し、ただし、サーバ識別子6302はチケット有効判定手段334のほかチケット更新指示手段631にも送られ、有効通知6303はチケット更新指示手段631及び第2の乱数生成手段632に送られる。チケット更新指示手段631は、有効通知6303が与えられると、チケット識別子3305とサーバ識別子6302と利用回数6301とを連結して認証チケット履歴更新指示データ6304を生成し、第3の送受信手段331を介して認証チケット履歴更新指示Update603として認証チケット管理手段64に送る（ST6302）とともに、利用回数6301をそのまま利用回数6306として第3の多段ハッシュ手段336へ送る。認証チケット管理手段64は、認証チケット履歴更新指示Update603が与えられた場合に、チケット識別子を用いてチケットリスト中を検索し、対応する有効回数を示す値が、対応する残り利用可能回数を示す値と認証チケット履歴更新指示Update603がともなう利用回数との合計に一致することをチェックして、正しければチケットリスト中の残り利用可能回数を示す値を1減じ、正し  
なければ認証チケット拒絶通知Reject606を送り返す。認証チケット拒絶通知606は認可サーバ手段63において、第3の送受信手段331を介して認証チケット拒絶通知データ6305として前記チケット更新指示手段631に送られる。チケット更新指示手段631は、多段ハッシュ値3306をそのまま多段ハッシュ値3312として認可照合手段337に送るが、認証チケット拒絶通知データ6305が与えられるとこれを抑止する。第2の乱数生成手段632は、有効通知6303が与えられると、データ攪乱用のチャ  
レンジ乱数6307を新たにランダムに生成して第2の排他  
的論理和手段633に送るとともに、第3の送受信手段331  
を介して認可チャレンジChallenge604としてクライアント  
手段61に送る（ST6303）。

【0154】これに対してクライアント手段61においては、認可チャレンジChallenge604は第1の送受信手段311で受信され、チャレンジ乱数6103が取出されて第1の排他  
的論理和手段612に送られる（ST6104）。多  
段ハッシュ手段317は、利用認可手順起動通知6101が与  
えられている場合に、前記機密記憶手段316よりハッシ

ュ値3113を得て、ハッシュ値3113に有効回数3112と利用  
回数6102との差に相当する段数のハッシュ演算Hを行な  
って、結果の多段ハッシュ値6104を、第1の排他的論理  
和手段612に送る。第1の排他的論理和手段612は、利用  
認可手順起動通知6101が与えられている場合に、多段ハ  
ッシュ値6104とチャレンジ乱数6103との間でビット毎の  
排他的論理和演算を行ない、攪乱多段ハッシュ値6105を  
生成し、第1の送受信手段311を介して認可チャレンジ  
応答Response605として認可サーバ手段63に送る（ST  
6105、ST6106）。ハッシュ演算Hが充分安全  
な方向性と結果の長さ及びランダム性を持っている限  
り、この攪乱多段ハッシュ値6105はパスワードPW、乱  
数R0及びチャレンジ乱数を知らない第三者には計算す  
ることができないため、この攪乱多段ハッシュ値6105に  
よりパスワードPWを知る正当なユーザであることが示  
される。また、過去にさかのぼるほど多段ハッシュ値に  
おけるハッシュ演算Hの段数が多く行なわれているた  
め、この多段ハッシュ値6104から次の多段ハッシュ値を  
計算することもできないので、暗号化の必要もない。な  
お、ハッシュ演算は一般に暗号演算よりも100倍以上  
高速であるとされ、適切な段数であれば暗号を用いた場  
合よりも高速に処理が行なえる。

【0155】これに対して認可サーバ手段63において  
は、認可チャレンジ応答Response605は第3の送受信手  
段331で受信され、攪乱多段ハッシュ値6308が取出され  
て第2の排他的論理和手段633に送られる（ST630  
4）。第2の排他的論理和手段633は、チャレンジ乱数6  
307と攪乱多段ハッシュ値6308との間でビット毎の排他  
的論理和演算を行なって、多段ハッシュ値6309を得て第  
3の多段ハッシュ手段336に送る（ST6305）。第  
3の多段ハッシュ手段336は、多段ハッシュ値6309に利  
用回数6306に相当する段数のハッシュ演算を行なって、  
結果の二次多段ハッシュ値3314を認可照合手段337に送  
る。認可照合手段337は図5、図6の場合と同様に動作  
し、認可通知データ3315を第3の送受信手段331を介し  
て認可通知Result308としてクライアント手段61に送  
り、クライアント手段61において受信される。ただし、  
認証チケット拒絶通知Reject606の受信により多段ハッ  
シュ値3312の供給が抑止された場合にはこの限りではな  
い（ST6306、ST6307）。この方法により、  
クライアント手段61はパスワードPWを認可サーバ手段  
63を含めた第三者に明かすことなく、n回まで認証チケ  
ット305を使用して複数の認可サーバ手段に対して利用  
認可を得ることができる。

【0156】なお、以上の説明ではクライアント手段61  
において利用認可手順のたびに多段ハッシュ値を計算す  
る構成としたが、認証チケットの取得時にすべての段数  
の多段ハッシュ値を事前計算して機密記憶手段316に記  
憶する構成としても良い。その場合、機密記憶手段316  
としてより大容量の耐タンパ性メモリデバイスを用いる

必要があるものの、利用認可手順ごとの処理時間をより短くすることができる。

【0157】このように、この実施形態では、認証チケットが更新されない方式の下で、認証チケットを複数の認可サーバに対して共通に用いることができる、利便性の高いシングルサインオン型の認証システムを構成することができる。

【0158】（第8の実施の形態）第8の実施形態の認証システムは、認証チケットの利用を分散管理することができる。

【0159】図20は、この認証システムのプロトコルを示すプロトコルシーケンス図である。図20において図14と異なるのは、クライアント手段71、認証サーバ手段72及び認可サーバ手段73であって、さらに第2の認可サーバ手段74を追加している。また、認可要求Authorize Request701が利用回数 $k$ をとともなう点、認可要求Authorize Request701及び認証チケットTicket305を受けた認可サーバ手段73が認可要求Authorize Request701及び認証チケット305から取出したチケット識別子TIDとサーバ識別子SIDと利用回数 $k$ をとともなった認証チケット履歴照会Inquiry702を認証サーバ手段72または第2の認可サーバ手段74へ送る点、これに対して必要に応じて認証チケット拒絶通知Reject705が返される点、認可チャレンジChallenge703が利用回数 $k$ の代わりに毎回異なるよう生成された乱数 $R_k$ をとともなう点、認可チャレンジ応答Response704がパスワードPWと乱数 $R_0$ との連結に対して $n-k+1$ 段のハッシュ演算 $H$ を施した結果にさらに $R_k$ との排他的論理和演算を行なった結果をとともなう点が異なる。

【0160】この方法により、クライアント手段71はパスワードPWを認可サーバ手段73、第2の認可サーバ手段74を含めた第三者に明かすことなく、 $n$ 回まで認証チケット304や更新された認証チケット501を使用して利用認可を得ることができ、利用回数 $k$ をクライアント手段71から認可サーバ手段73を介して認証チケットを発行した認証サーバ手段72または更新した第2の認可サーバ手段74に送ってチェックするため、認証チケット304を複数の認可サーバ手段73、74で共通に利用可能なものとして、かつチェック処理のトラフィックを分散化できる。

【0161】このようなプロトコルシーケンスを持つ認証システムの構成について図21を参照しながら説明する。図21においても図15と異なるのは、クライアント手段71、認証サーバ手段72、認可サーバ手段73であって、さらに第2の認可サーバ手段74を追加している。また、クライアント手段71において図15のクライアント手段51と異なるのは、認証チケットを保持するとともにその利用回数 $k$ を管理するチケット保持管理手段711をチケット保持手段511の代わりに設け、ビット毎の排他的論理和演算を行なう第1の排他的論理和手段712を設

け、一部の結線を改めた点にある。また、認証サーバ手段72において図15の認証サーバ手段32と異なるのは、認証チケットの発行を管理して照会に回答するチケット発行管理手段721を設け、一部の結線を改めた点にある。また、認可サーバ手段73において図15の認可サーバ手段53と異なるのは、認証チケットのチケット識別子と有効回数と残り利用可能回数とを受取って各部に供給するとともに認証チケットの更新を管理して照会に回答するチケット更新管理手段731をチケット利用管理手段531の代わりに設け、利用認可処理毎に乱数を生成する第2の乱数生成手段732、ビット毎の排他的論理和演算を行なう第2の排他的論理和手段733を設け、一部の結線を改めた点にある。第2の認可サーバ手段74は認可サーバ手段73と同様の構成を持つものである。

【0162】チケット保持管理手段711としては、チケット保持手段511と同様の構成に利用回数の計算を行なう加算回路を追加して使用できる。第1、第2の排他的論理和手段712、733としては、例えば論理回路が使用できる。チケット発行管理手段721としては、例えばデータの分割結合を行なう論理回路と利用回数を照合する演算回路及び比較回路と大容量のメモリデバイスとの組合せにより構成できる。チケット更新管理手段731としては、例えばデータの分割結合を行なう論理回路と利用回数を照合する演算回路及び比較回路と大容量のメモリデバイスとの組合せにより構成できる。第2の乱数生成手段732としては、乱数生成手段324と同様の構成が使用できる。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【0163】以上のように構成された認証システムの動作について図22を参照しながら説明する。ここでは、認証要求Authenticate Request301が認証チケット有効回数 $n$ をとともなう場合について説明する。

【0164】まず、ユーザ認証手順におけるクライアント手段71及び認証サーバ手段72における動作は図15、図16の場合とほぼ同様で、最終的には認証サーバ手段72よりクライアント手段71へ認証チケットTicket304が送られる。ただし、クライアント手段71においては、このときのチケット保持手段511の動作をチケット保持管理手段711が行なう。また認証サーバ手段72においては、認証要求Authenticate Request301から取出された有効回数7201は多段ハッシュ手段325及び認証子付加手段328のほかチケット発行管理手段721にも送られ、サーバ識別子7202は認証子付加手段328のほかチケット発行管理手段721にも送られ、チケット識別子生成手段327で生成されたチケット識別子7203は認証子付加手段328のほかチケット発行管理手段721にも送られる。チケット



発行管理手段721は発行したチケットリストを管理しており、チケット識別子7203とサーバ識別子7202と有効回数7201と残り利用可能回数を示す値としての有効回数7201の組をチケットリストに追加し記憶する（ST7201）。

【0165】これに対してクライアント手段71においては、認証チケットTicket304は第1の送受信手段311で受信され、認証チケットデータ3110が取出されて前記チケット保持管理手段711に送られる。前記チケット保持管理手段711は、認証チケットデータ3110をサーバ識別子3101と対応づけて保持し、認証チケットデータから取出した有効回数を残り利用可能回数として同時に管理し（ST7101）、利用認可手順起動通知7101が与えられた場合に、認証チケットデータ3111を第1の送受信手段311を介して認証チケットTicket305として、また、残り利用可能回数を1減じたうえで認証チケットから取出した有効回数から引くことにより得た利用回数7102を（ST7102）第1の送受信手段311を介して認可要求Authorize Request701として、それぞれ認可サーバ手段73に送り（ST7103）、さらに認証チケットデータから取出した有効回数3112を多段ハッシュ手段317に送る。

【0166】これに対して認可サーバ手段73においては、認証チケットTicket305及び認可要求Authorize Request701は第3の送受信手段331で受信され、認証チケットデータ3301が取出されて認証子検証手段333に送られ、利用回数7301が取出されてチケット更新管理手段731に送られる（ST7301）。

【0167】認可計時手段332、認証子検証手段333及びチケット有効判定手段334は図15、図16の場合とほぼ同様に動作し、ただし、サーバ識別子7302はチケット有効判定手段334のほかチケット更新管理手段731にも送られ、有効通知7303はチケット更新管理手段731及び第2の乱数生成手段732に送られる。チケット更新管理手段731は発行したチケットリストを管理しており、有効通知7303が与えられると、チケット識別子3305とサーバ識別子7302と利用回数7301とを連結して認証チケット履歴照会データ7304を得て、第3の送受信手段331を介して発行者識別子3308の示す認証サーバ手段72または第2の認可サーバ手段74へ認証チケット履歴照会Inquiry702を送るとともに、チケット識別子3305とサーバ識別子7302と有効回数7301と残り利用可能回数を示す値としての有効回数7301の組をチケットリストに追加し記憶する（ST7302）。

【0168】これを受けた認証サーバ手段72では、認証チケット履歴照会Inquiry702は第2の送受信手段321で受信され、チケット識別子とサーバ識別子と利用回数とを含んだ認証チケット履歴照会データ7205として前記チケット発行管理手段721に送られる。前記チケット発行管理手段721は、認証チケット履歴照会データ7205から

取出した利用回数が、自ら管理する有効回数と残り利用可能回数との差に1加えたものと一致するかを調べ、不一致の場合には認証チケット拒絶通知データ7204を第2の送受信手段321を介して認証チケット拒絶通知Reject705として送り返す。なお、第2の認可サーバ手段74がこれを受けた場合には、チケット更新管理手段が前記チケット発行管理手段721と同様の役割を行なう。

【0169】認可サーバ手段73においては、認証チケット拒絶通知705は第3の送受信手段331を介して認証チケット拒絶通知データ7305として前記チケット更新管理手段731に送られる。前記チケット更新管理手段731は、多段ハッシュ値3306をそのまま多段ハッシュ値5302として認可照合手段337に送り、チケット識別子と残り利用可能回数とサーバ識別子との組5303を第2の認証子付加手段533に送るが、認証チケット拒絶通知データ7305が与えられるとこれらを抑止する。第2の乱数生成手段732は、有効通知7303が与えられると、データ攪乱用のチャレンジ乱数7306を新たにランダムに生成して第2の排他的論理和手段733に送るとともに、第3の送受信手段331を介して認可チャレンジChallenge703としてクライアント手段71に送る（ST7303）。

【0170】これに対してクライアント手段71においては、認可チャレンジChallenge703は第1の送受信手段311で受信され、チャレンジ乱数7103が取出されて第1の排他的論理和手段712に送られる（ST7104）。多段ハッシュ手段317は、利用認可手順起動通知7101が与えられている場合に、前記機密記憶手段316よりハッシュ値3113を得て、ハッシュ値3113に有効回数3112と利用回数7102との差に相当する段数のハッシュ演算Hを行なって、結果の多段ハッシュ値7104を、第1の排他的論理和手段712に送る。第1の排他的論理和手段712は、利用認可手順起動通知7101が与えられている場合に、多段ハッシュ値7104とチャレンジ乱数7103との間でビット毎の排他的論理和演算を行ない、攪乱多段ハッシュ値7105を生成し、第1の送受信手段311を介して認可チャレンジ応答Response704として認可サーバ手段73に送る（ST7105、ST7106）。ハッシュ演算Hが充分安全な一方方向性と結果の長さ及びランダム性を持っている限り、この攪乱多段ハッシュ値7105はパスワードPW、乱数R0及びチャレンジ乱数を知らない第三者には計算することができないため、この攪乱多段ハッシュ値7105によりパスワードPWを知る正当なユーザであることが示される。また、過去にさかのぼるほど多段ハッシュ値におけるハッシュ演算Hの段数が多く行なわれているため、この多段ハッシュ値7104から次の多段ハッシュ値を計算することもできないので、暗号化の必要もない。なお、ハッシュ演算は一般に暗号演算よりも100倍以上高速であるとされ、適切な段数であれば暗号を用いた場合よりも高速に処理が行なえる。

【0171】これに対して認可サーバ手段73において

は、認可チャレンジ応答Response704は第3の送受信手段331で受信され、攪乱多段ハッシュ値7307が取出されて第2の排他的論理和手段733に送られる（ST7304）。第2の排他的論理和手段733は、チャレンジ乱数7306と攪乱多段ハッシュ値7307との間でビット毎の排他的論理和演算を行なって、多段ハッシュ値7308を得て第3のハッシュ手段532に送る（ST7305）。第3のハッシュ手段532は、多段ハッシュ値7308にハッシュ演算を行なって、結果の二次多段ハッシュ値5305を認可照合手段337に送る。認可照合手段337及び第2の認証子付加手段533は図15、図16の場合と同様に動作し、認証チケットデータ5308を第3の送受信手段331を介して認証チケットTicket501としてクライアント手段71に送る。ただし、認証チケット拒絶通知Reject705の受信により多段ハッシュ値5302及びチケット識別子と残り利用可能回数とサーバ識別子との組5303の供給が抑止された場合にはこの限りではない（ST7306、ST7307）。

【0172】これに対してクライアント手段71においては、認証チケットTicket501は第1の送受信手段311で受信され、認証チケットデータ5101として前記チケット保持管理手段711に送られ保持されて（ST7107、ST7108）、次の利用認可手順で使用される。

【0173】これによりクライアント手段71から認可サーバ手段73に送られる認証チケット305がともなう攪乱多段ハッシュ値は、その段数が利用認可ごとに1ずつ減っていくので、認可サーバ手段73ではハッシュ演算は1段のみ行なえば良く、応答時間が短縮できる。また、タイムスタンプが更新されるため有効期限をアクセスの間隔をカバーできる程度の短さ、例えば1時間に設定でき、ユーザ利便性は低下させずに安全性を高めることができる。この方法により、クライアント手段71はパスワードPWを認可サーバ手段73、74を含めた第三者に明かすことなく、安全性のより高い認証チケット305を使用してn回まで、より短い応答時間で利用認可を得ることができ、その認証チケットは複数の認可サーバで共通に利用可能で、かつチェック処理のトラフィックを分散化できる。

【0174】なお、以上の説明ではクライアント手段71において利用認可手順のたびに多段ハッシュ値を計算する構成としたが、認証チケットの取得時にすべての段数の多段ハッシュ値を事前計算して機密記憶手段316に記憶する構成としても良い。その場合、機密記憶手段316としてより大容量の耐タンパ性メモリデバイスを用いる必要があるものの、利用認可手順ごとの処理時間をより短くすることができる。

【0175】このように、認証システムを本実施形態のように構成することにより、認証チケットが更新される方式の下で、認証チケットの利用を分散管理することができる。そのため、1個所の管理リソースをより少なくで

きる。

【0176】

【発明の効果】以上の説明から明らかなように、本発明では、第1に、クライアント側での暗号処理を必要とせず、認証チケットの使用回数を容易に管理して二重使用を排除することができる、シングルサインオン型の認証方法及び認証システムが得られる。

【0177】第2に、ユーザ認証手順においても、クライアント側での暗号処理を必要としないという、認証提示情報の演算処理と提示情報の演算処理とが共通化できる、シングルサインオン型の認証方法及び認証システムが得られる。

【0178】第3に、クライアント手段が生成した認証用乱数を秘密情報として照合情報を生成するものでは、認証チケットが含む照合情報がユーザ認証情報と無関係となるため認証チケットからユーザ認証情報が推測される可能性すらなく、より安全性の高いシングルサインオン型の認証方法及び認証システムが得られる。

【0179】第4に、秘密情報の不可逆演算を一方向性ハッシュ演算で行なうことにより、クライアント側が計算処理能力の低い装置であっても実用的な処理時間で利用認可処理を行なうことができる、シングルサインオン型の認証方法及び認証システムが得られる。

【0180】第5に、認可サーバ手段が認証チケットの照合情報等を更新するものでは、認証チケットが使用することに更新され、特にタイムスタンプが更新されるため有効判定における有効期限をより短く設定できるので、第三者による不正使用の可能性をより小さくでき、さらに利用認可の応答時間を短縮できる、シングルサインオン型の認証方法及び認証システムが得られる。

【0181】第6に、認証チケットの使用回数を管理する認証チケット管理手段を設けたものでは、認証チケットが更新されないシステムにおいて、認証チケットを複数の認可サーバに対して共通に用いることが可能となるため、より利便性の高いシングルサインオン型の認証方法及び認証システムが得られる。

【0182】第7に、認証サーバ手段や認可サーバ手段が認証チケットの発行履歴を記憶するものでは、認証チケットが更新されるシステムにおいて、認証チケットの利用を分散管理できるため1個所の管理リソースをより少なくできる、シングルサインオン型の認証方法及び認証システムが得られる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態における認証システムの概要を示す概念図、

【図2】本発明の第2の実施の形態における認証システムの概要を示す概念図、

【図3】本発明の第3の実施の形態における認証システムの概要を示す概念図、

【図4】本発明の第4の実施の形態における認証システ

ムのプロトコルシーケンス図、

【図5】本発明の第4の実施の形態における認証システムの機能ブロック図、

【図6】本発明の第4の実施の形態における認証システムの動作を示すフロー図、

【図7】本発明の第4の実施の形態における認証システムにおいてメッセージ認証コードを用いた場合の認証子付加手段の詳細な機能ブロック図、

【図8】本発明の第4の実施の形態における認証システムにおいてメッセージ認証コードを用いた場合の認証子検証手段の詳細な機能ブロック図、

【図9】本発明の第4の実施の形態における認証システムにおいてデジタル署名を用いた場合の認証子付加手段の詳細な機能ブロック図、

【図10】本発明の第4の実施の形態における認証システムにおいてデジタル署名を用いた場合の認証子検証手段の詳細な機能ブロック図、

【図11】本発明の第5の実施の形態における認証システムのプロトコルシーケンス図、

【図12】本発明の第5の実施の形態における認証システムの機能ブロック図、

【図13】本発明の第5の実施の形態における認証システムの動作を示すフロー図、

【図14】本発明の第6の実施の形態における認証システムのプロトコルシーケンス図、

【図15】本発明の第6の実施の形態における認証システムの機能ブロック図、

【図16】本発明の第6の実施の形態における認証システムの動作を示すフロー図、

【図17】本発明の第7の実施の形態における認証システムのプロトコルシーケンス図、

【図18】本発明の第7の実施の形態における認証システムの機能ブロック図、

【図19】本発明の第7の実施の形態における認証システムの動作を示すフロー図、

【図20】本発明の第8の実施の形態における認証システムのプロトコルシーケンス図、

【図21】本発明の第8の実施の形態における認証システムの機能ブロック図、

【図22】本発明の第8の実施の形態における認証システムの動作を示すフロー図、

【図23】従来の認証方法の概要を示す概念図、

【図24】従来の認証方法のプロトコルシーケンス図、

【図25】従来の認証方法の機能ブロック図、

【図26】従来の認証方法の動作を示すフロー図である。

【符号の説明】

1、11、21、31、41、51、61、71、81 クライアント手段

2、12、22、32、42、62、72、82 認証サーバ手段

3、33、53、63、73、83 認可サーバ手段

4、14、24 秘密情報

5、7、803、805 認証チケット

6、804 提示情報

8、806 認可通知

13、23、801 認証提示情報

64 認証チケット管理手段

74 第2の認可サーバ手段

311 第1の送受信手段

312、811 入力手段

313 ハッシュ手段

314 チケット保持手段

316 機密記憶手段

317 多段ハッシュ手段

321 第2の送受信手段

322 認証計時手段

323 認証情報蓄積手段

324 乱数生成手段

325 第2の多段ハッシュ手段

326 認証照合手段

327 チケット識別子生成手段

328 認証子付加手段

328A 自識別子記憶手段

328B データ連結手段

328C 連結データハッシュ手段

328D サーバ共通鍵記憶手段

328E 共通鍵方式暗号手段

328F 認証子連結手段

328G 自秘密鍵記憶手段

328H 公開鍵方式暗号手段

331 第3の送受信手段

332 認可計時手段

333 認証子検証手段

333A 認証子分離手段

333B 第2の連結データハッシュ手段

333C 第2のサーバ共通鍵記憶手段

333D 第2の共通鍵方式暗号手段

333E データ分離手段

333F 発行者識別子照合手段

333G 比較手段

333H サーバ公開鍵蓄積手段

333J 公開鍵方式復号手段

334、832 チケット有効判定手段

335、531 チケット利用管理手段

336 第3の多段ハッシュ手段

337 認可照合手段

411 認証用乱数生成手段

412、612、712 第1の排他的論理和手段

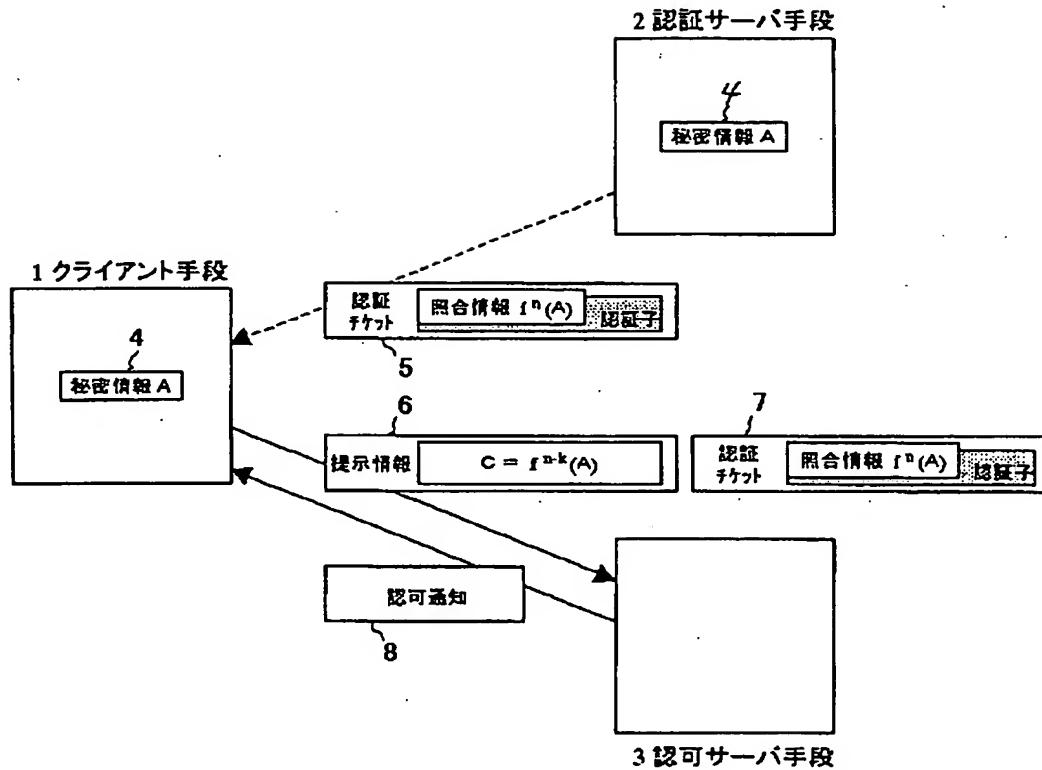
421 第2のハッシュ手段

422 第2の排他的論理和手段

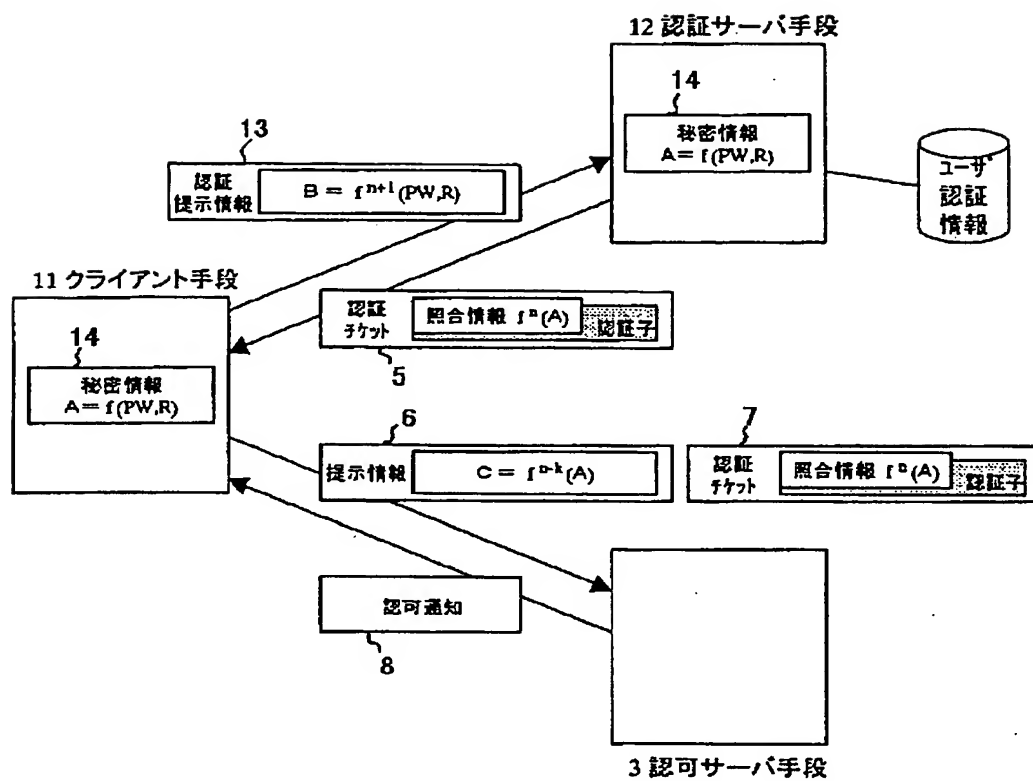
423 第2の多段ハッシュ手段  
 511 チケット保持手段  
 532 第3のハッシュ手段  
 533 第2の認証子付加手段  
 611、711 チケット保持管理手段  
 621 チケット登録指示手段  
 631 チケット更新指示手段  
 632 第2の乱数生成手段  
 633、733 第2の排他的論理和手段  
 721 チケット発行管理手段  
 731 チケット更新管理手段

732 第2の乱数生成手段  
 812 セッション鍵復号手段  
 813 証明計時手段  
 814 証明情報暗号手段  
 821 セッション鍵生成手段  
 822 セッション鍵暗号手段  
 823 チケット暗号手段  
 831 チケット復号手段  
 833 証明情報復号手段  
 10 834 証明情報有効判定手段  
 835 認可照合手段

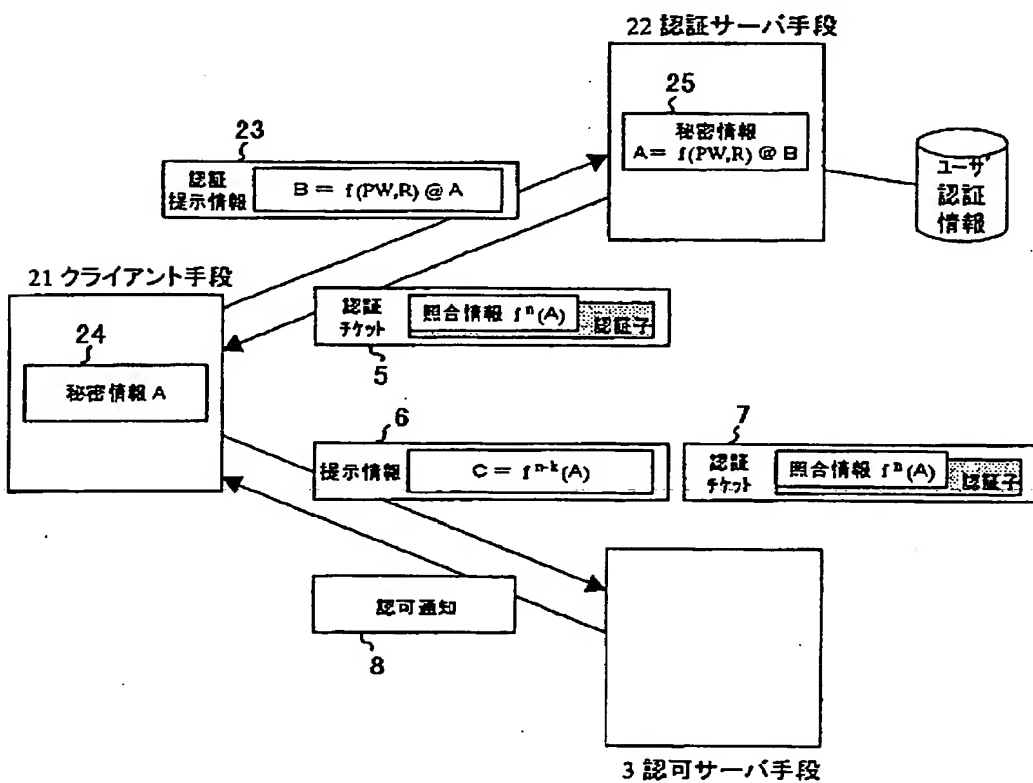
【図1】



【図2】

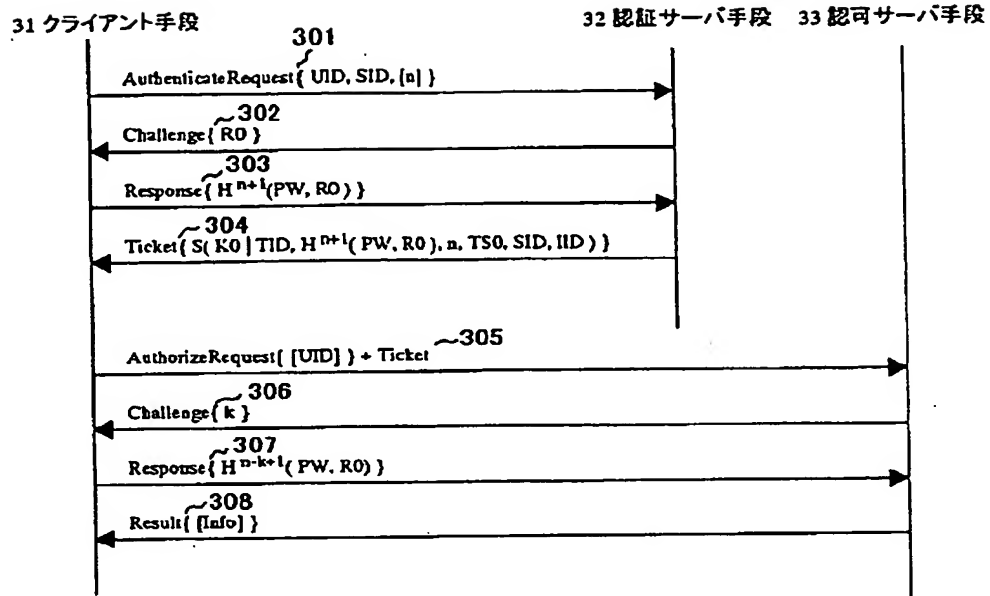


【図3】

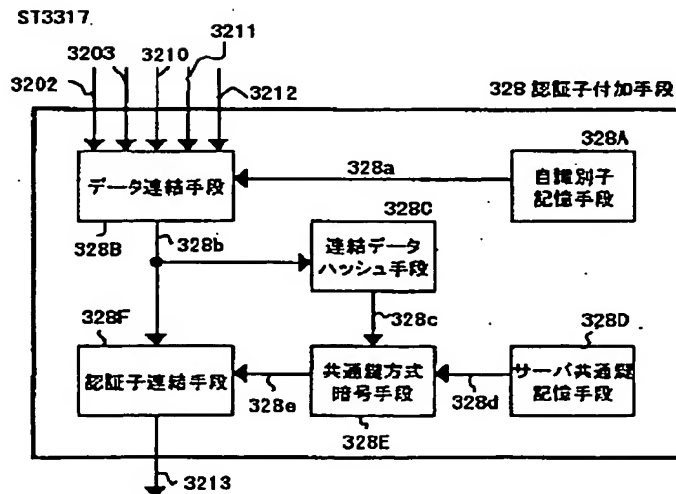




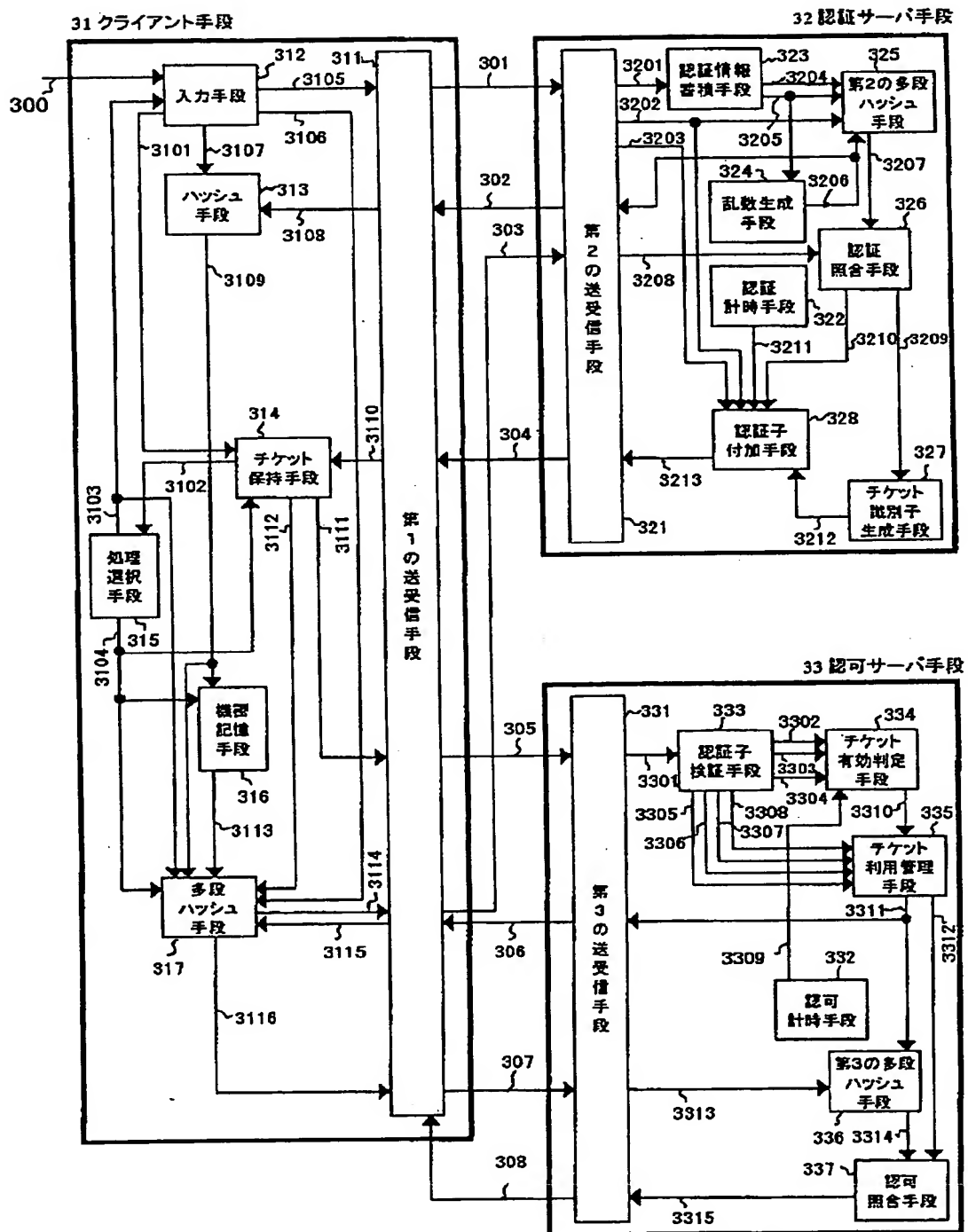
【図4】



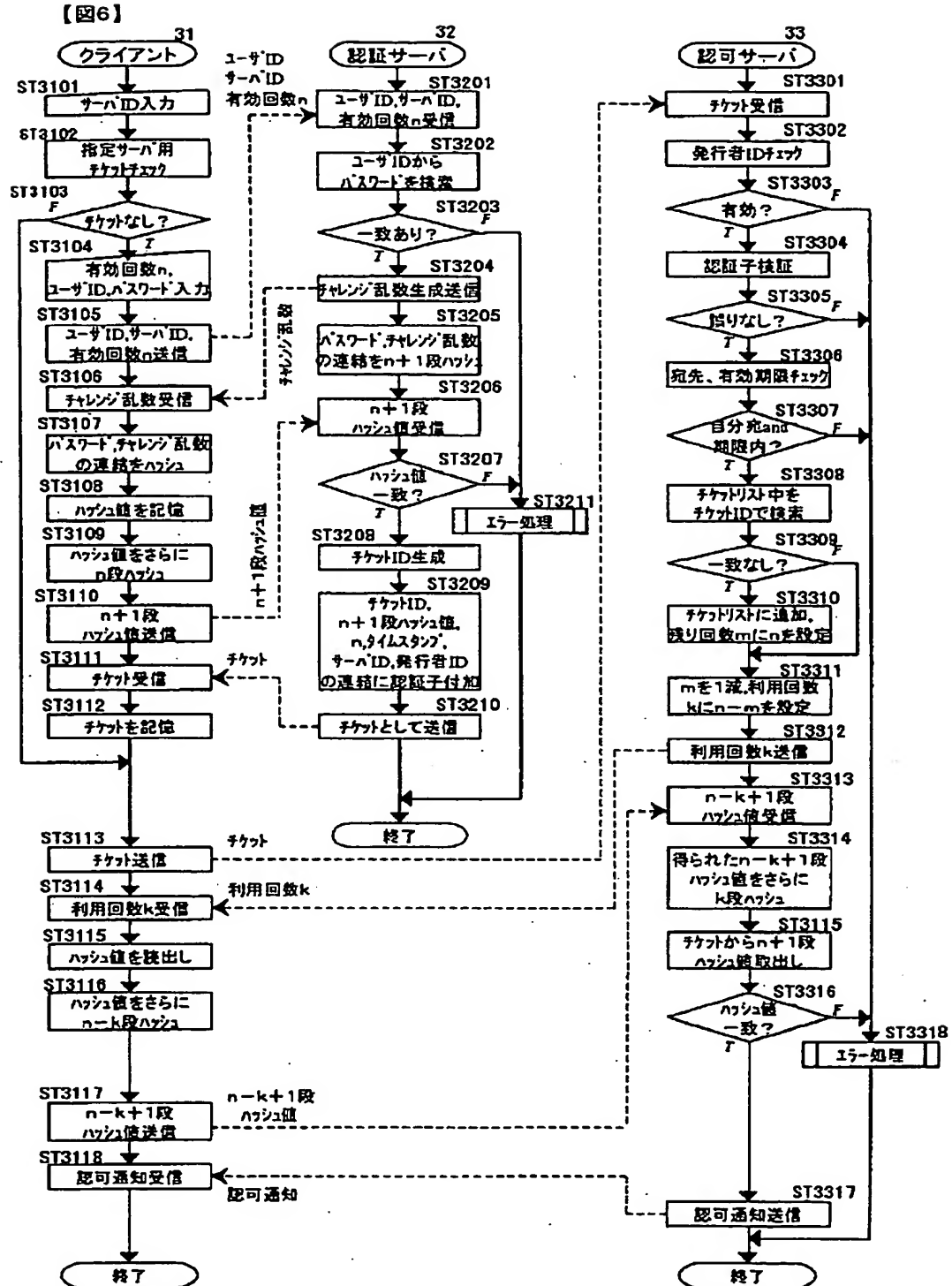
【図7】



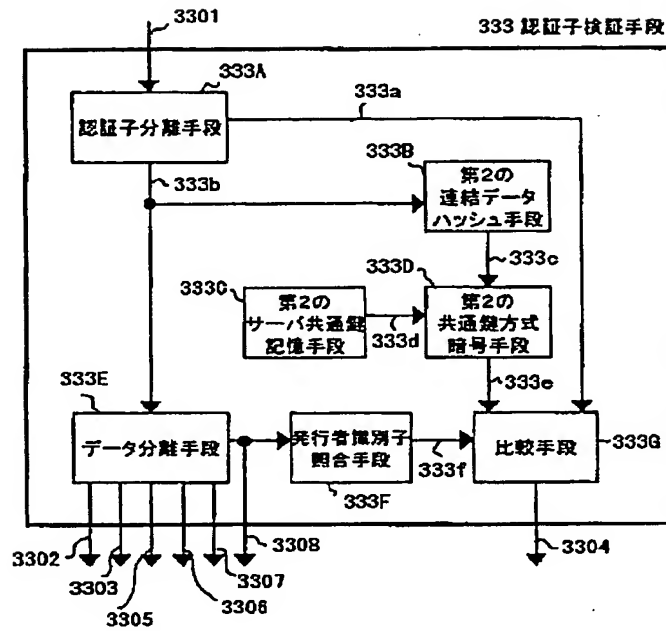
【图 5】



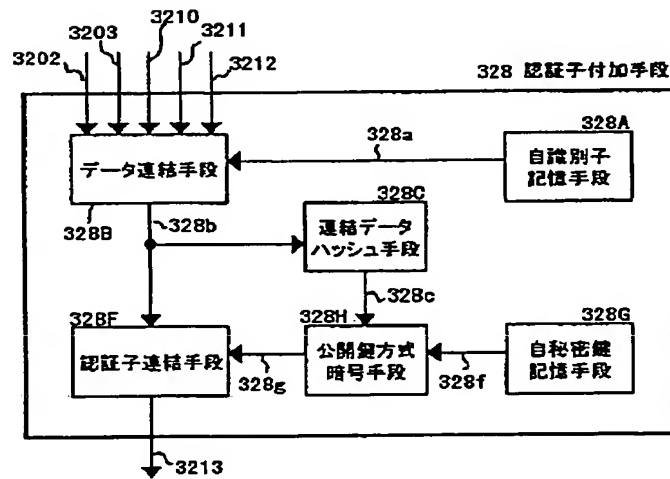
【図6】



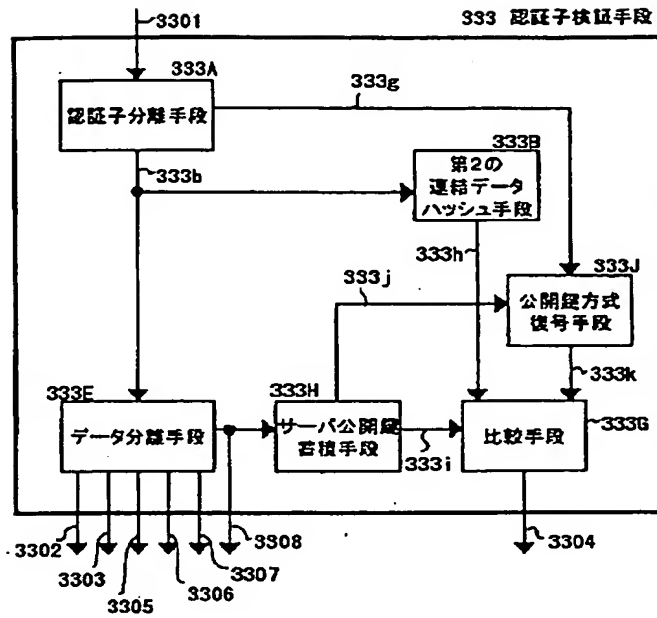
【図8】



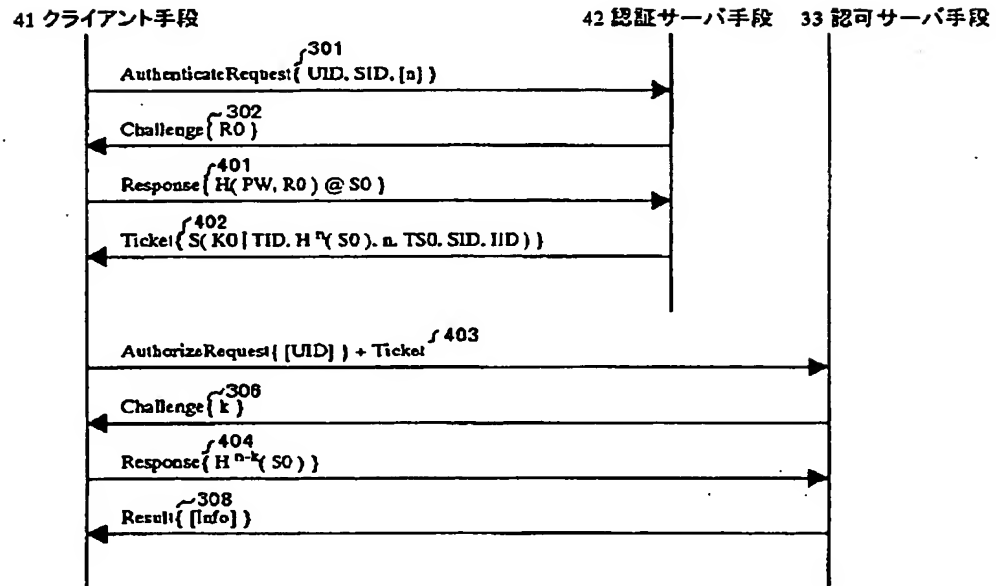
【図9】



【図10】

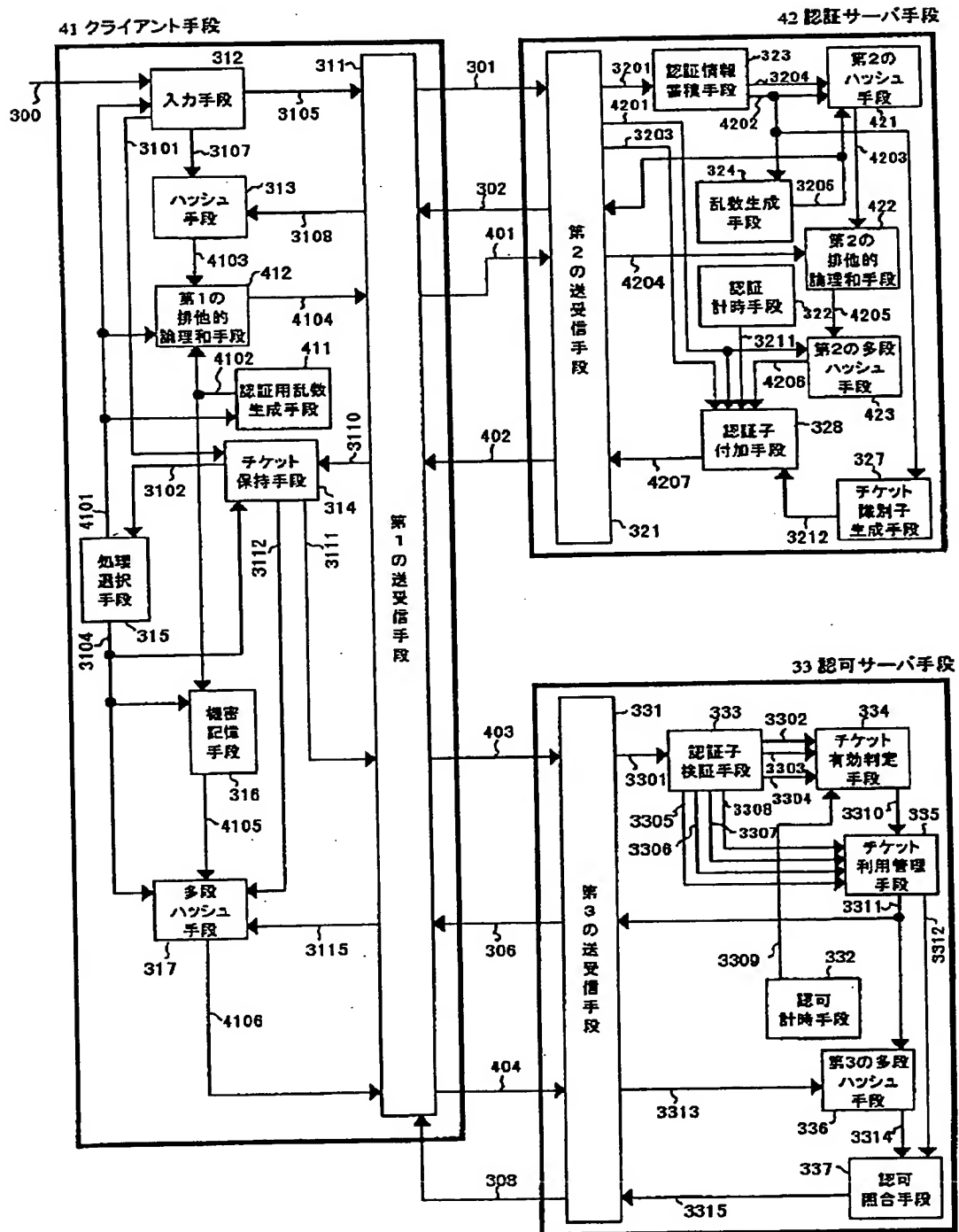


【図11】

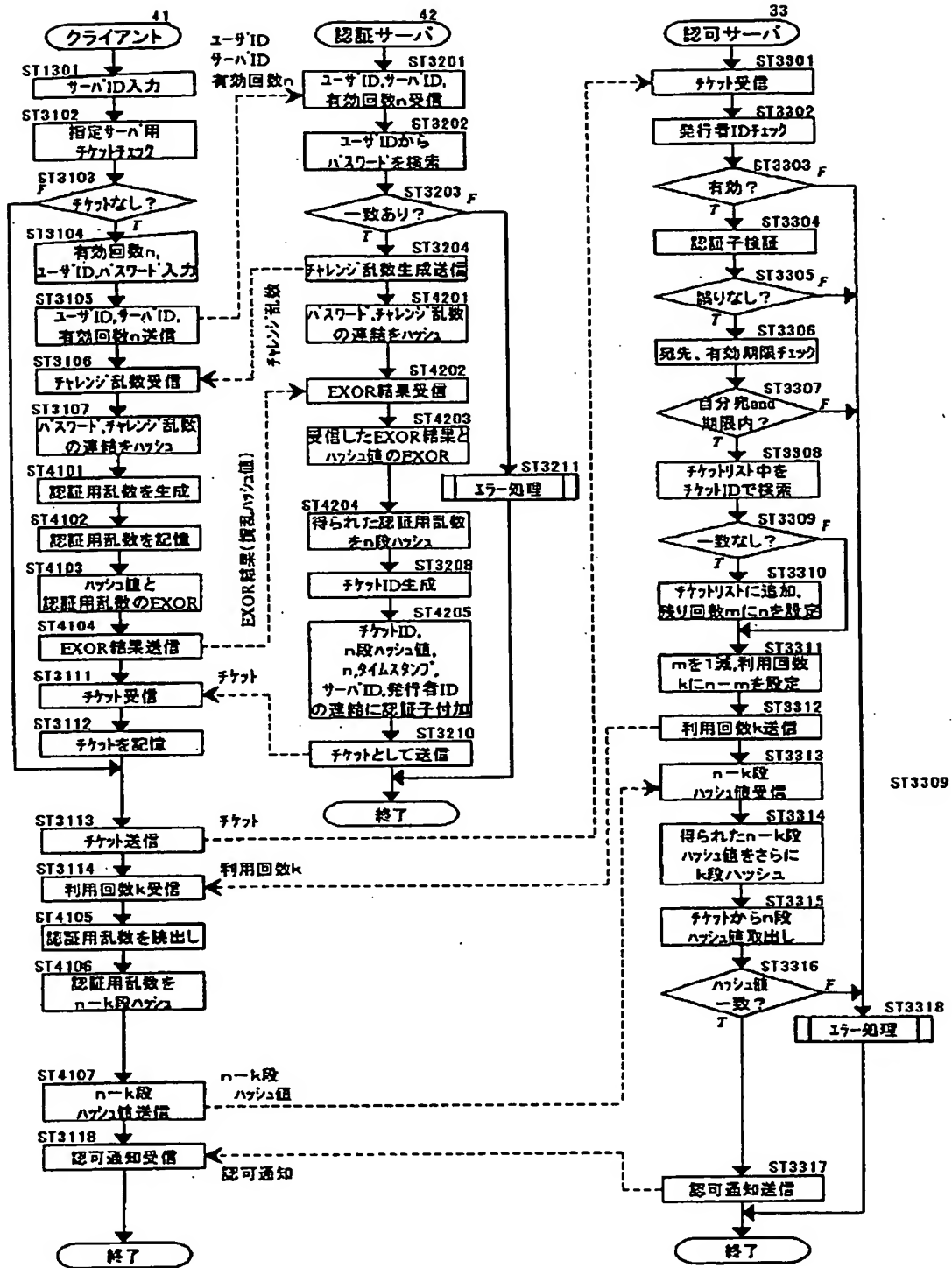




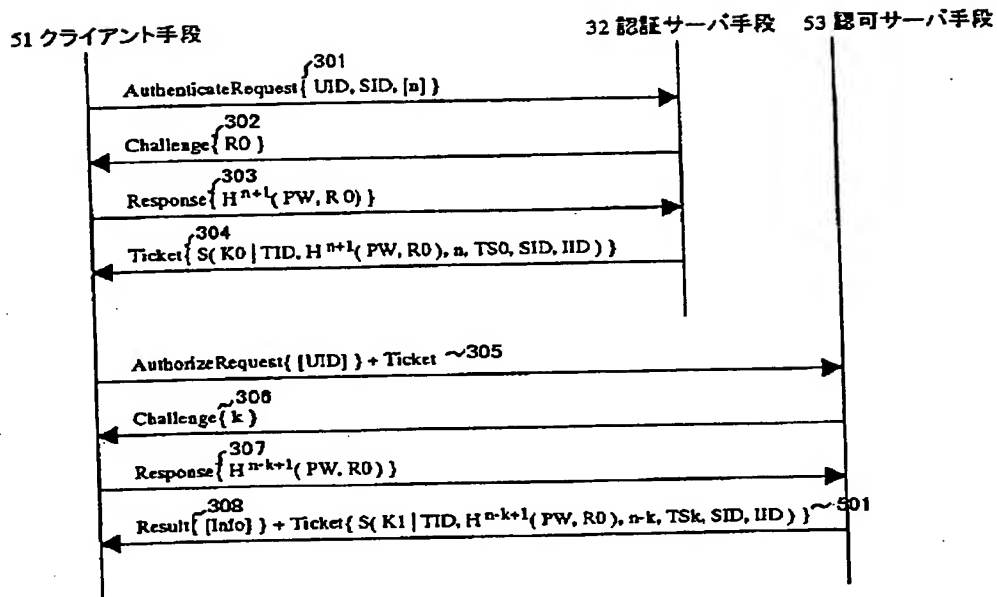
【図12】



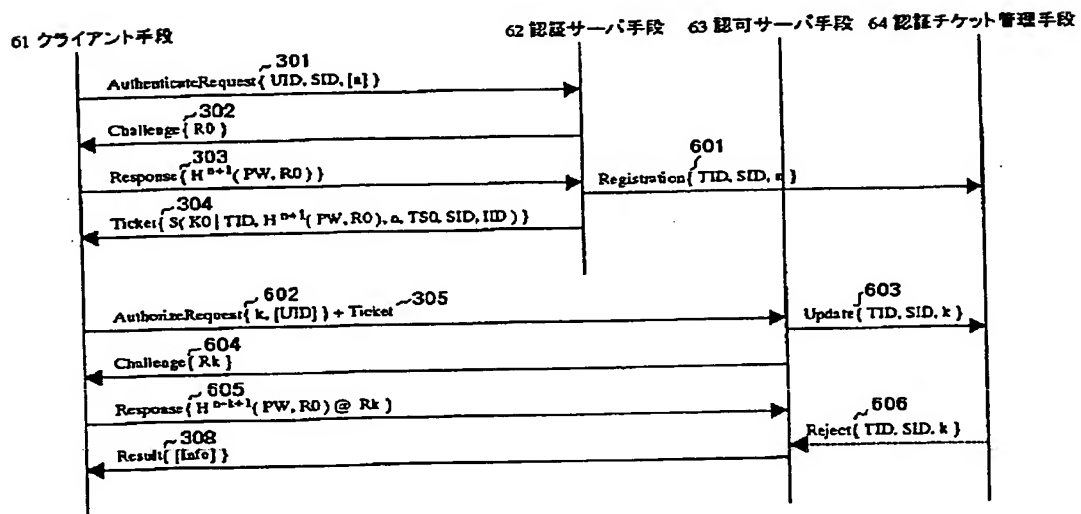
【図13】



【図14】



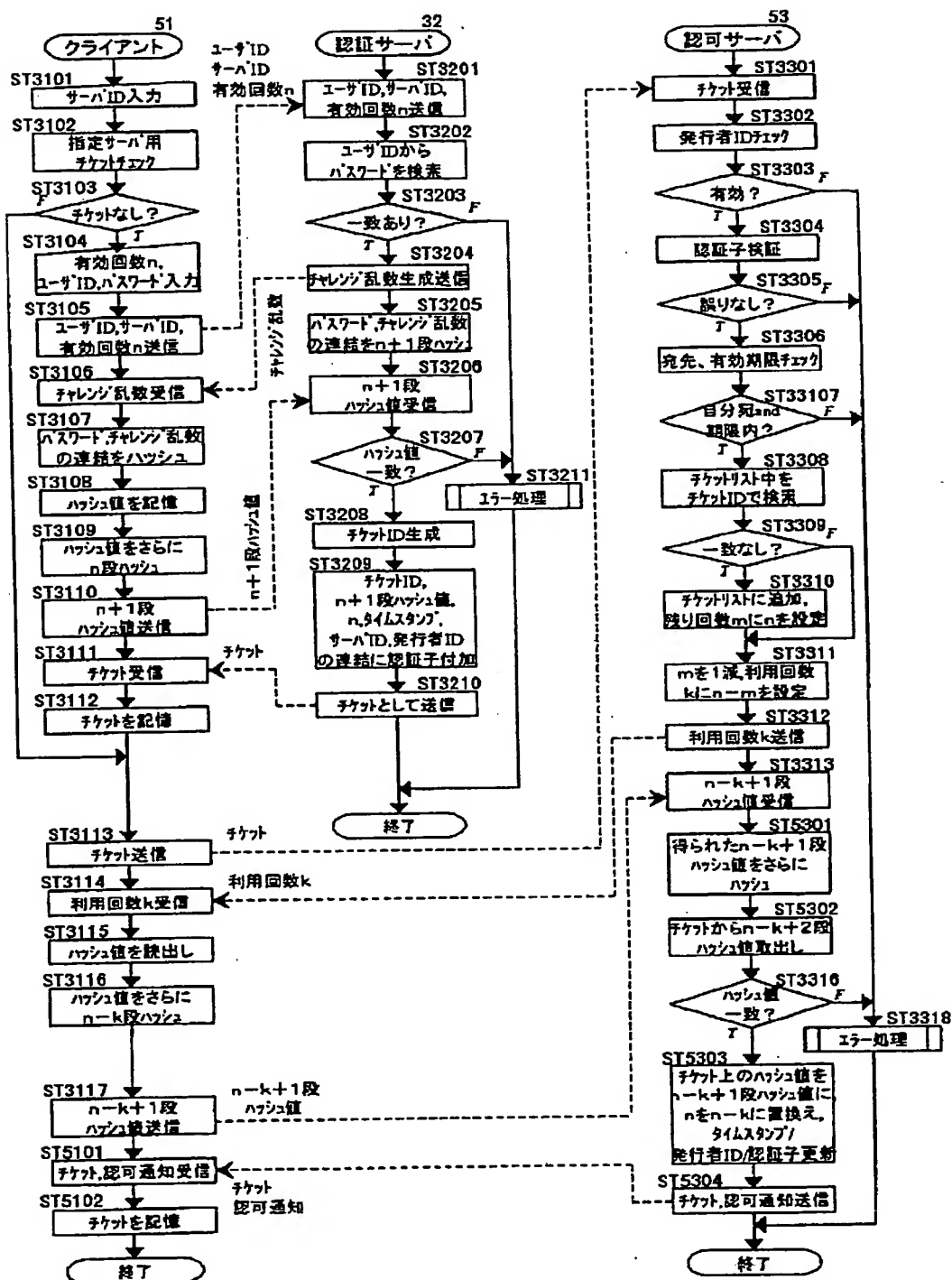
【図17】



-37-

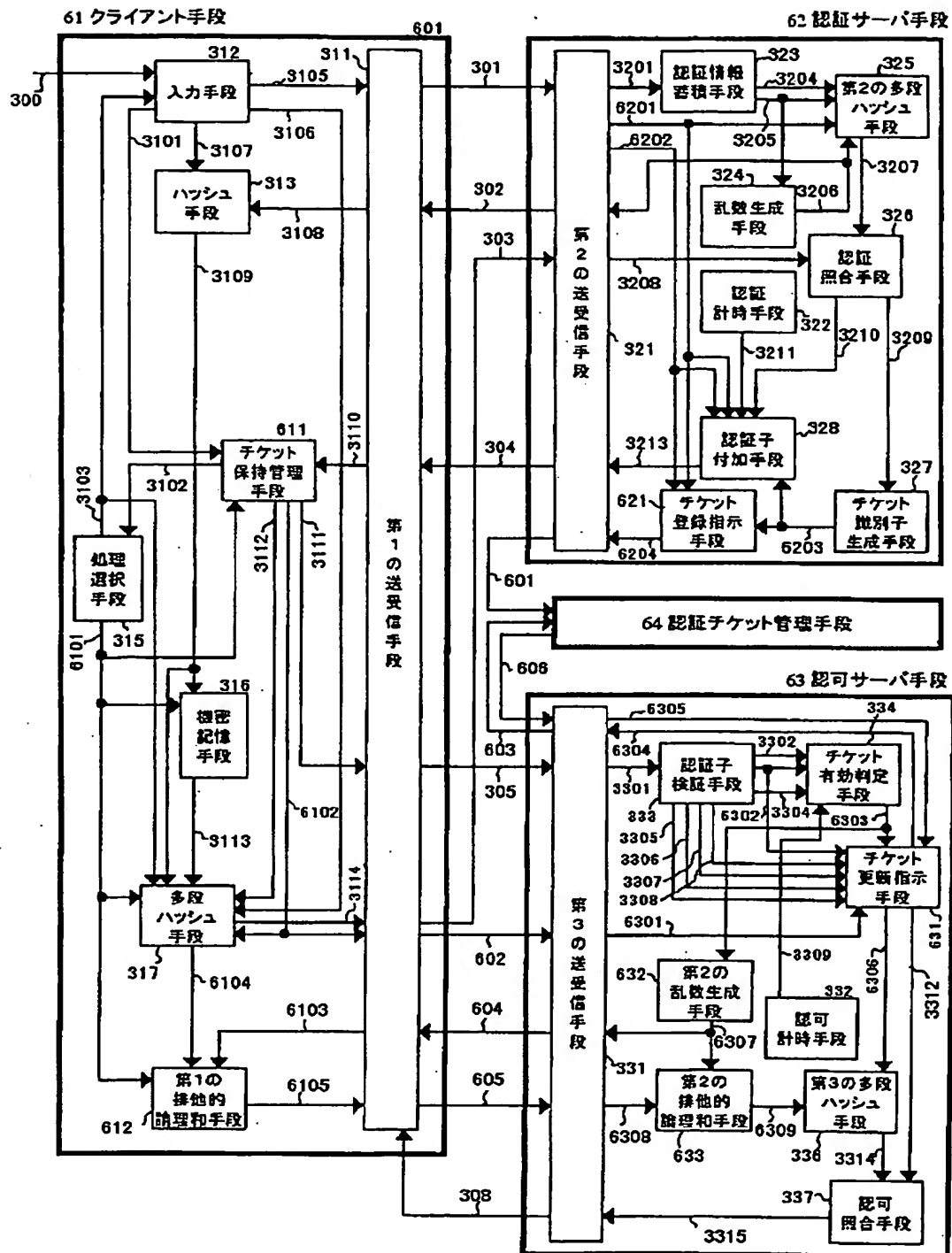


【図16】

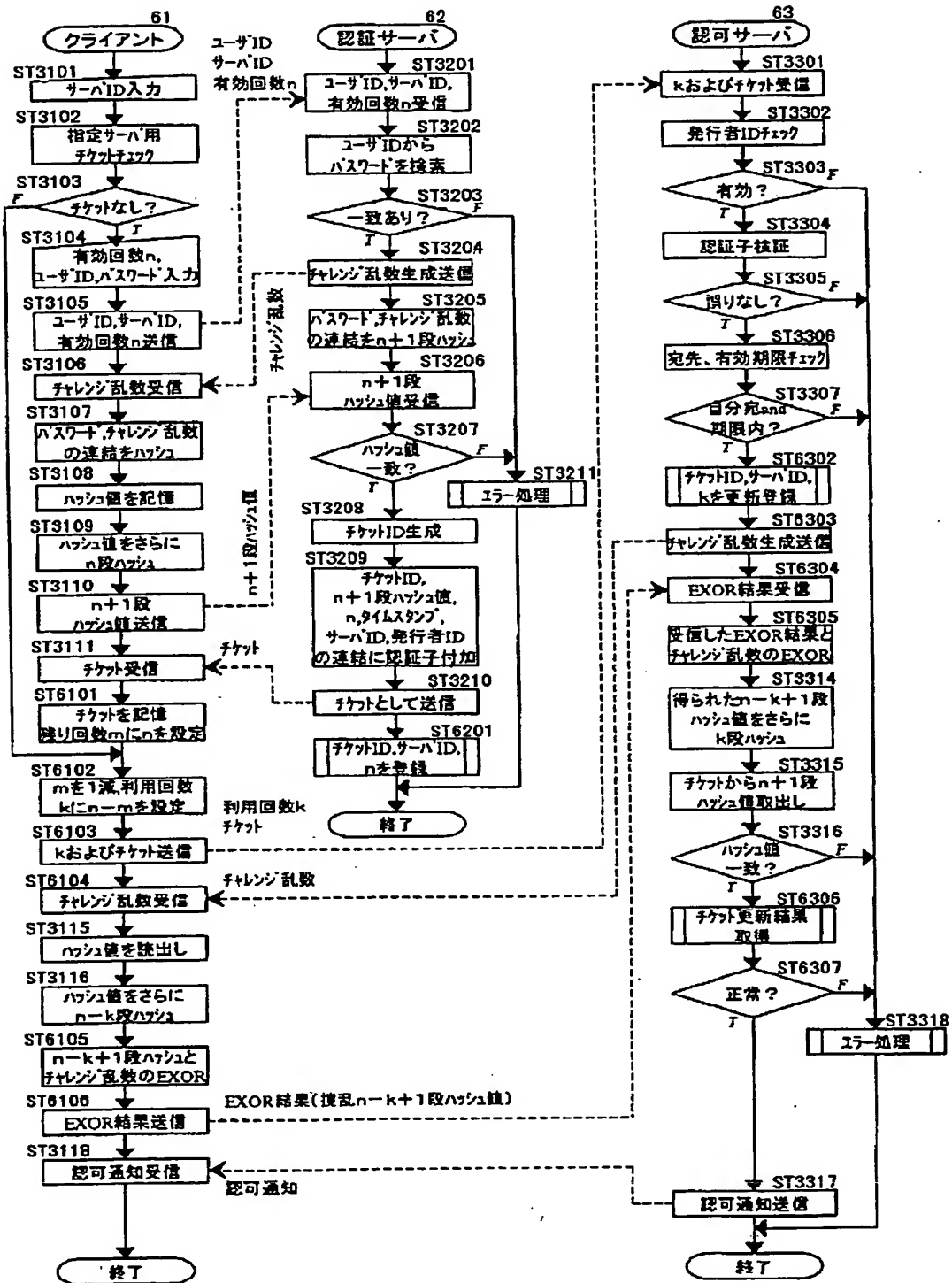




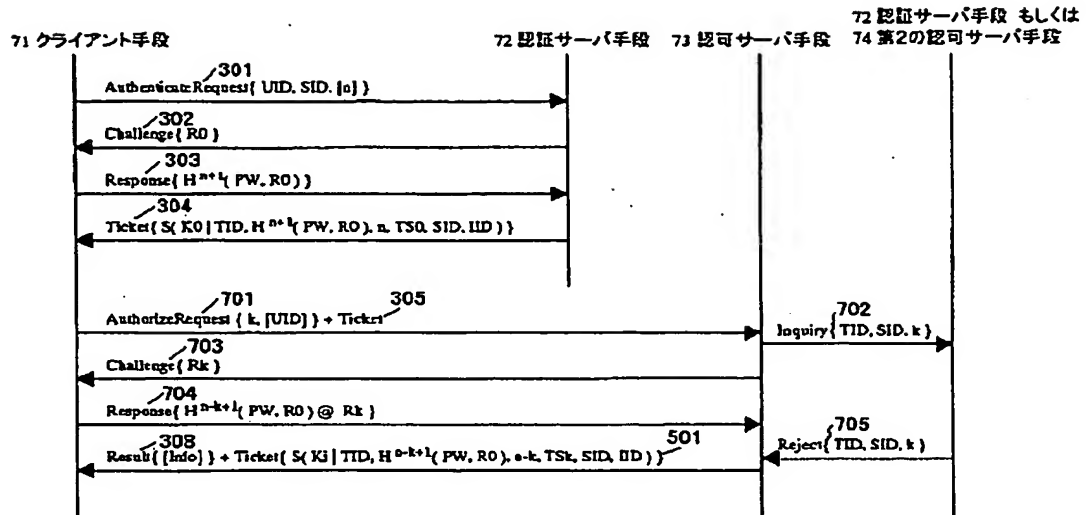
【図18】



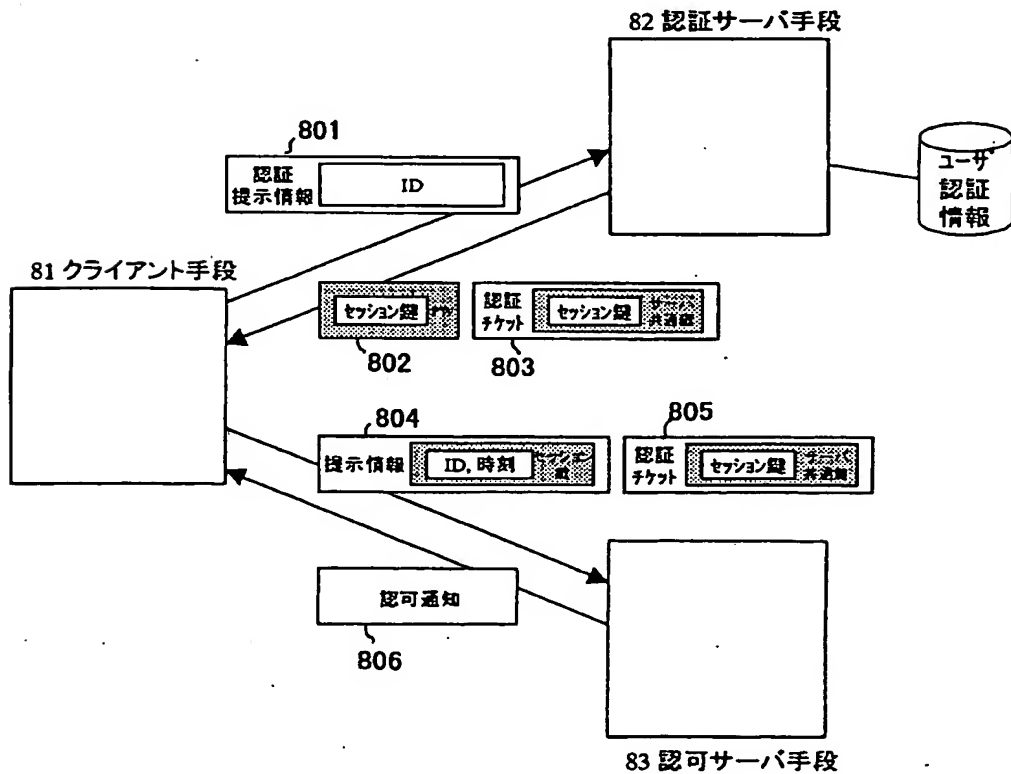
【图 19】



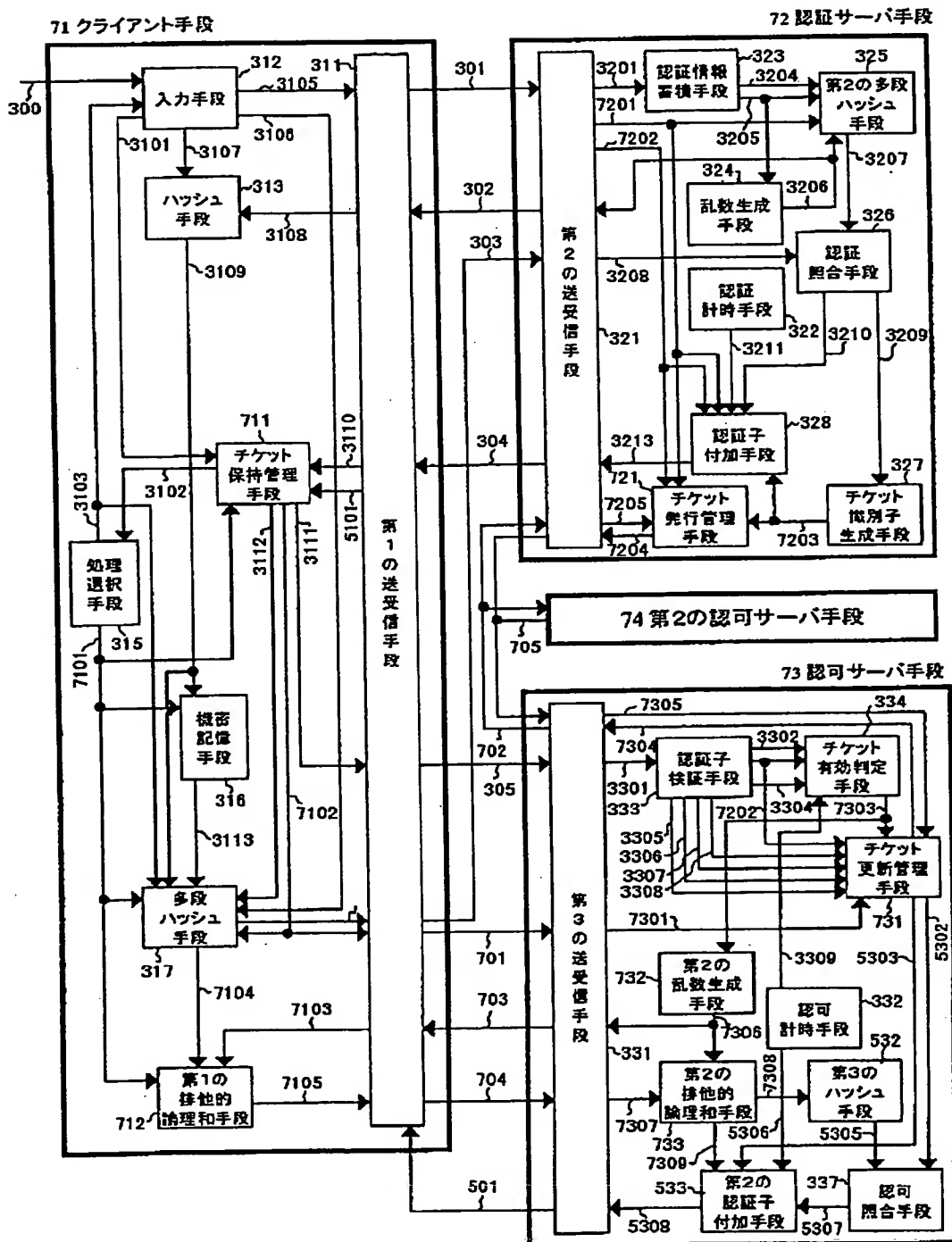
【図20】



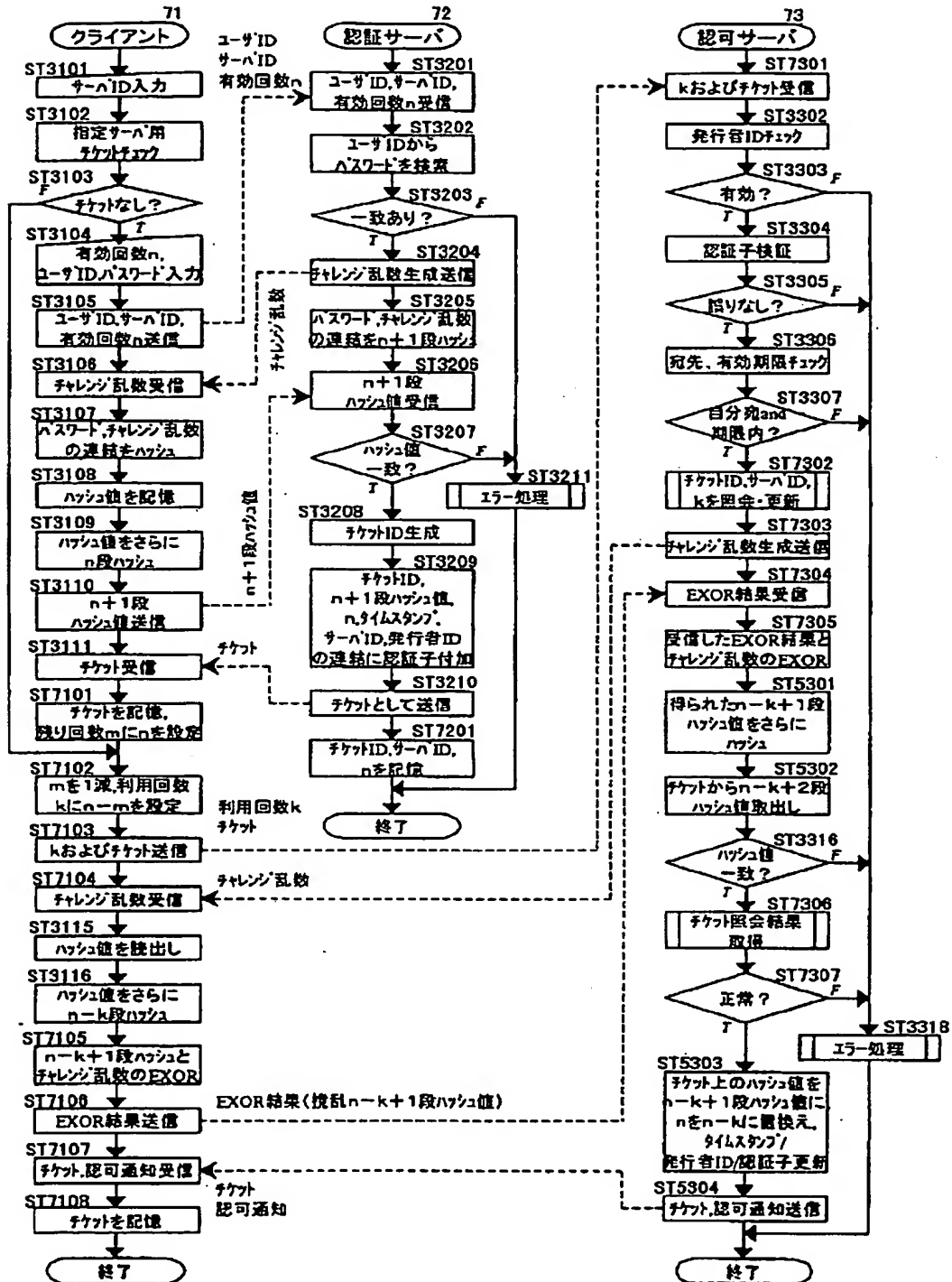
【図23】



【図21】

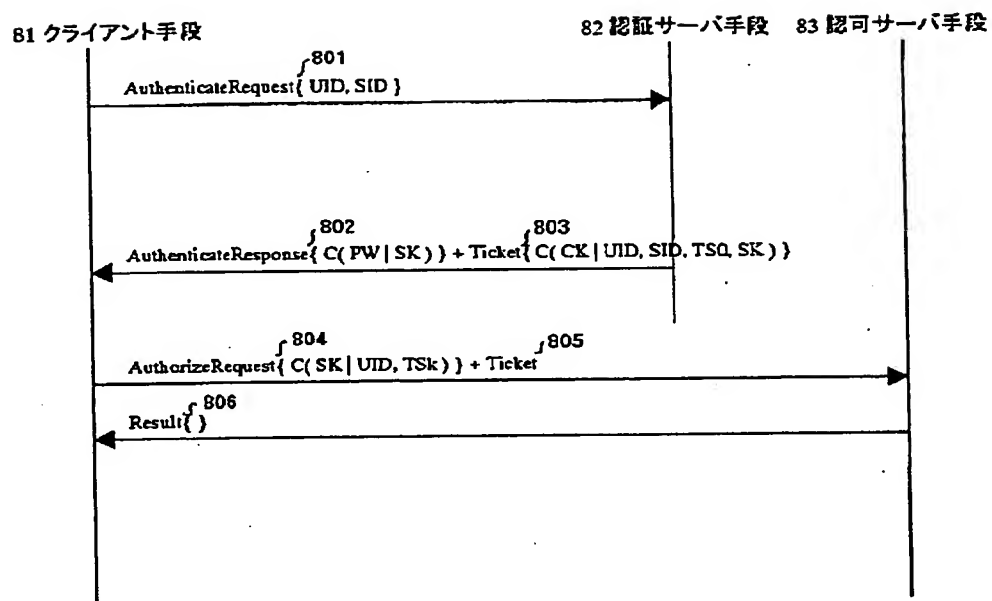


【図22】

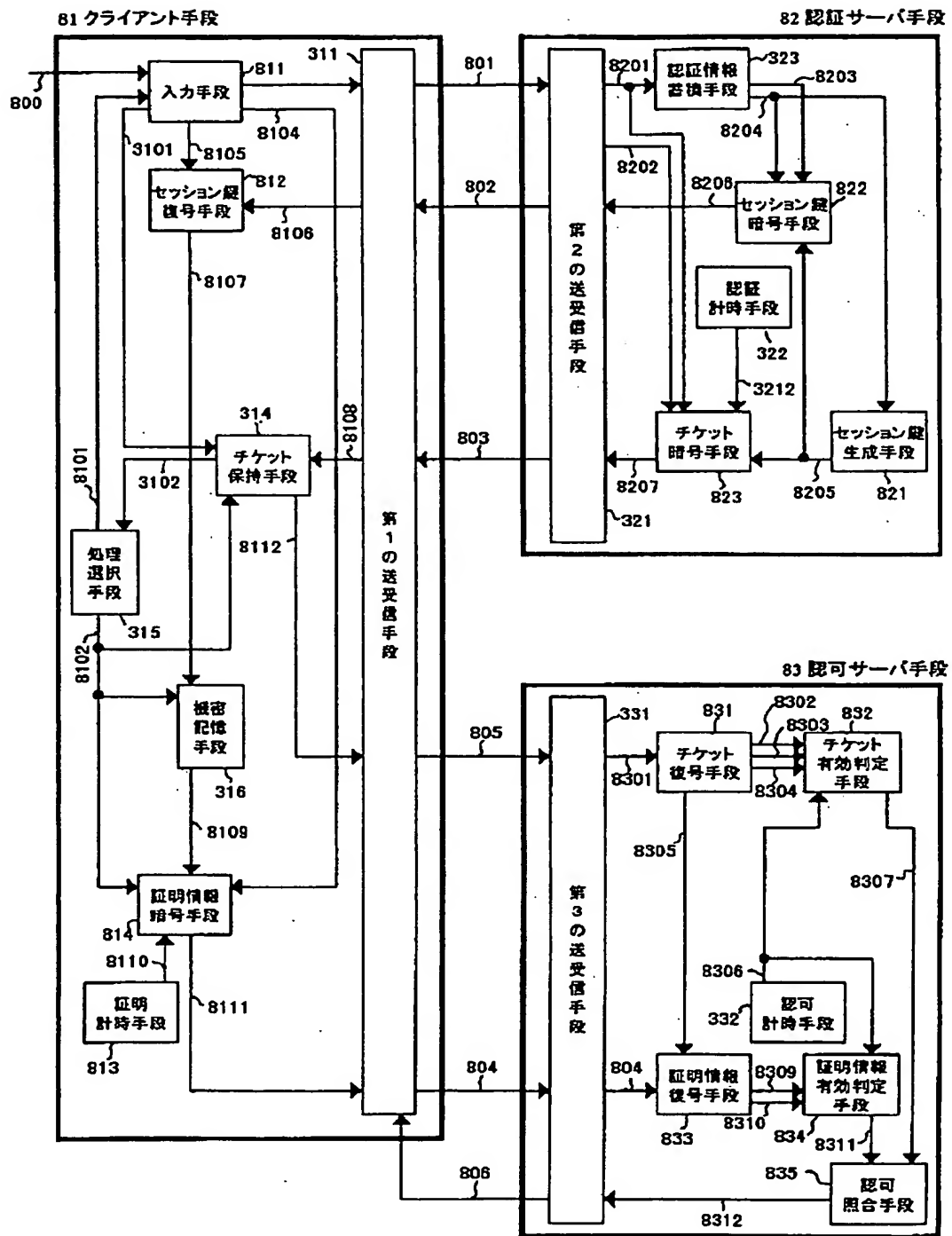




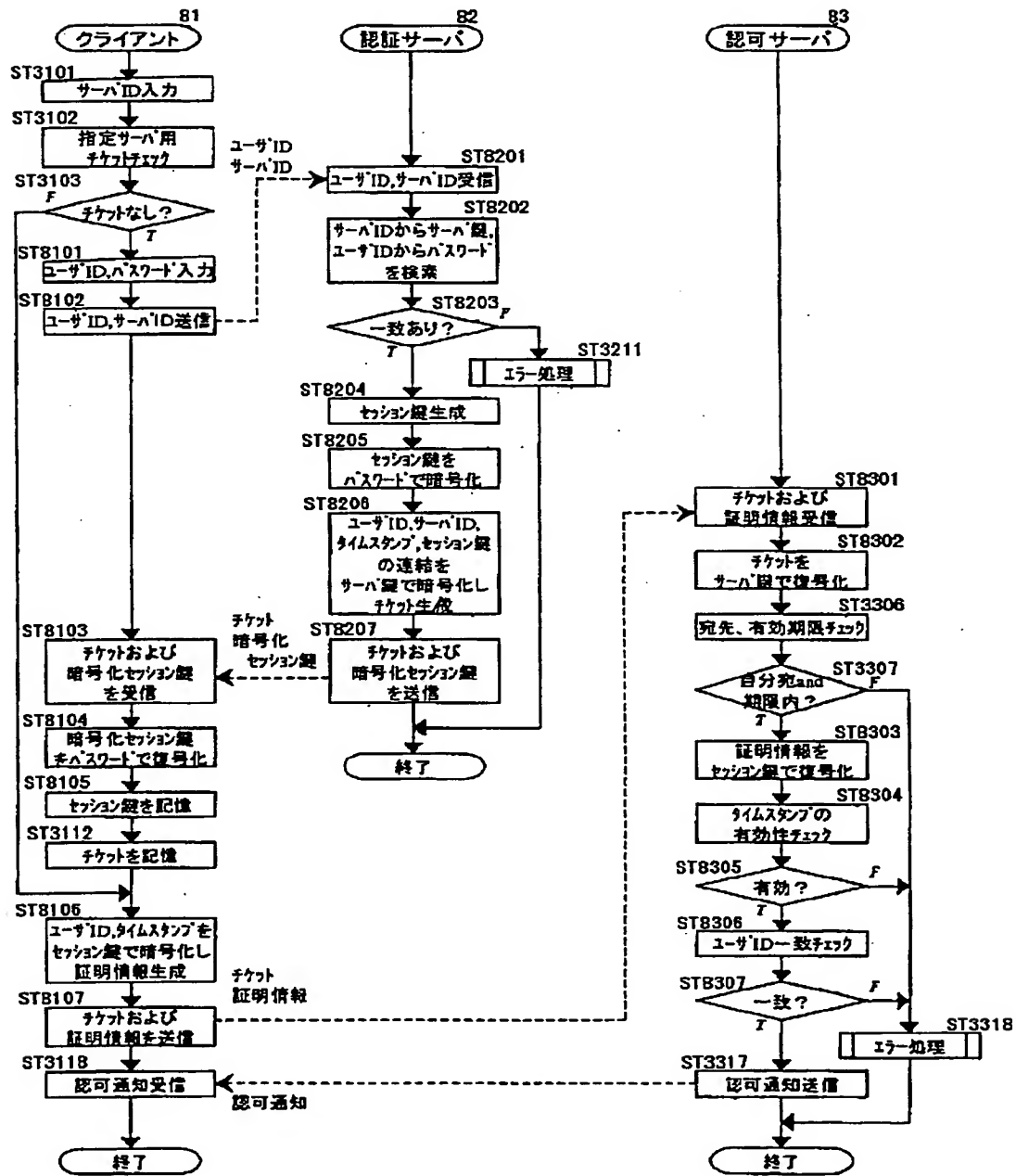
【図24】



【図25】



【図26】



【手続補正書】

【提出日】平成11年2月2日(1999.2.2)

【手続補正1】

【補正対象書類名】図面

【補正対象項目名】図25

【補正方法】変更

【補正内容】

【図25】



## フロントページの続き

F ターム(参考) 5B017 AA01 AA07 BA05 BA07 BB03  
BB07 BB10 CA16  
5B058 KA33 KA40  
5B085 AE01 AE06 AE09 AE13 AE23  
BC01 BG07  
5B089 GA11 GA21 GB03 KA17 KB13  
KC58  
5J104 AA07 KA01 KA04 PA07